AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TESTING AND CERTIFICATION FOR VOTING EQUIPMENT: HOW CAN THE PROCESS BE IMPROVED?

HEARING

BEFORE THE

SUBCOMMITTEE ON ENVIRONMENT, TECHNOLOGY, AND STANDARDS

COMMITTEE ON SCIENCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 24, 2004

Serial No. 108–65

Printed for the use of the Committee on Science

Available via the World Wide Web: http://www.house.gov/science

U.S. GOVERNMENT PRINTING OFFICE

94–316PS WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON SCIENCE

HON. SHERWOOD L. BOEHLERT, New York, *Chairman*

RALPH M. HALL, Texas
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
GIL GUTKNECHT, Minnesota
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
MELISSA A. HART, Pennsylvania
J. RANDY FORBES, Virginia
PHIL GINGREY, Georgia
ROB BISHOP, Utah
MICHAEL C. BURGESS, Texas
JO BONNER, Alabama
TOM FEENEY, Florida
RANDY NEUGEBAUER, Texas
VACANCY

BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
MICHAEL M. HONDA, California
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
SHEILA JACKSON LEE, Texas
ZOE LOFGREN, California
BRAD SHERMAN, California
BRIAN BAIRD, Washington
DENNIS MOORE, Kansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
DENNIS A. CARDOZA, California
VACANCY
VACANCY
VACANCY

SUBCOMMITTEE ON ENVIRONMENT, TECHNOLOGY, AND STANDARDS

VERNON J. EHLERS, Michigan, *Chairman*

NICK SMITH, Michigan
GIL GUTKNECHT, Minnesota
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
TIMOTHY V. JOHNSON, Illinois
MICHAEL C. BURGESS, Texas
VACANCY
SHERWOOD L. BOEHLERT, New York

MARK UDALL, Colorado
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
BRIAN BAIRD, Washington
JIM MATHESON, Utah
ZOE LOFGREN, California
BART GORDON, Tennessee

ERIC WEBSTER *Subcommittee Staff Director*
MIKE QUEAR *Democratic Professional Staff Member*
JEAN FRUCI *Democratic Professional Staff Member*
OLWEN HUXLEY *Professional Staff Member*
MARTY SPITZER *Professional Staff Member*
SUSANNAH FOSTER *Professional Staff Member*
AMY CARROLL *Professional Staff Member/Chairman's Designee*
ADAM SHAMPAINE *Majority Staff Assistant*
MARTY RALSTON *Democratic Staff Assistant*

CONTENTS

June 24, 2004

Appendix: Answers to Post-Hearing Questions

TESTING AND CERTIFICATION FOR VOTING EQUIPMENT: HOW CAN THE PROCESS BE IMPROVED?

THURSDAY, JUNE 24, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENVIRONMENT, TECHNOLOGY, AND STANDARDS,
COMMITTEE ON SCIENCE,
Washington, DC.

The Subcommittee met, pursuant to other business, at 2:20 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Vernon J. Ehlers [Chairman of the Subcommittee] presiding.

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Testing and Certification for Voting Equipment: How Can the Process be Improved?

Thursday June 24, 2004

2:00 PM – 4:00 PM
2318 Rayburn House Office Building (WEBCAST)

Witness List

Panel I

Representative Rush Holt
Member, U.S. House of Representatives

Panel II

Mr. Tom Wilkey
Chair
Independent Testing Authority (ITA) Committee
National Association of State Elections Directors (NASED)

Ms. Carolyn Coggins
Director
ITA services at SysTest Labs

Dr. Michael Shamos
Professor of Computer Science
Carnegie Mellon University

Dr. Hratch Semerjian
Acting Director
National Institute of Standards and Technology (NIST)

Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science strives to accommodate/meet the needs of those requiring special assistance. If you need special accommodation, please contact the Committee on Science in advance of the scheduled event (3 days requested) at (202) 225-6371 or FAX (202) 225-0891.

Should you need Committee materials in alternative formats, please contact the Committee as noted above.

HEARING CHARTER

SUBCOMMITTEE ON ENVIRONMENT, TECHNOLOGY, AND STANDARDS

COMMITTEE ON SCIENCE

U.S. HOUSE OF REPRESENTATIVES

Testing and Certification for Voting Equipment: How Can the Process Be Improved?

THURSDAY, JUNE 24, 2004
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

Purpose:

On Thursday, June 24, 2004, the House Science Subcommittee on Environment, Technology, and Standards will hold a hearing to examine how voting equipment is tested against voting system standards and how the independent laboratories that test voting equipment are selected.

Each election season, a small number of newly deployed voting machines fail to perform properly in the field, causing confusion in the polling places and concerns over the potential loss of votes. Because these machines have already been tested and certified against standards, these incidents have raised questions about the reliability of the testing process, the credibility of standards against which the machines are tested, and the laboratories that carry out the tests. While most of the national attention on voting systems has been focused on the subjects of computer hacking and voter-verifiable paper ballots, press reports (see Appendix A) have also highlighted the problems of voting machine testing.

A focus of the hearing will be how the implementation of the Help America Vote Act (HAVA) is intended to improve the way voting machines are tested, the role of the National Institute of Standards and Technology (NIST), and what changes can be implemented in time for the 2004 election and beyond.

Witnesses:

Dr. Hratch Semerjian—Acting Director, National Institute of Standards and Technology (NIST).

Mr. Tom Wilkey—Chair of the National Association of State Elections Directors (NASED) Independent Testing Authority (ITA) Committee. He is the former Executive Director of the New York State Board of Elections.

Ms. Carolyn Coggins—Director of Independent Testing Authority Services for SysTest Laboratories, a Denver laboratory that tests software used in voting machines.

Dr. Michael Shamos—Professor of Computer Science at Carnegie Mellon University. He has served as an Examiner of Electronic Voting Systems for Pennsylvania.

Overarching Questions:

The Subcommittee plans to explore the following questions:

- How are the accreditation of testing laboratories and the testing and certification of voting equipment conducted?
- How should voting equipment standards and laboratory testing be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?
- What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?

Background:

Introduction

In October 2002, Congress passed the Help America Vote Act (HAVA) to help correct the problems with voting machines that were brought to the public's attention during the 2000 federal election. Under HAVA, the States are receiving $2.3 billion in fiscal 2004 to purchase new voting equipment. To try to encourage and enable states to buy effective voting equipment, HAVA reformed the way standards for voting machines are developed and the way voting machines are tested against those standards. However, HAVA does not require any state or manufacturer to abide by the standards.

Before the passage of the Help America Vote Act (HAVA), the Federal Election Commission (FEC) established voting system standards. A non-governmental group of State elections directors (the National Association of State Elections Directors, or NASED) accredited the laboratories, also known as Independent Testing Authorities (ITAs), which then tested whether voting systems met the standards. With the passage of HAVA, the responsibility for issuing voting system standards and for accrediting the ITAs was transferred to the Election Assistance Commission (EAC). Under HAVA, the EAC is to select ITAs based on the recommendations of the National Institute of Standards and Technology (NIST). For more information on HAVA, see Appendix B.

The transition to the new standards regime, however, has been slow. Members of the EAC were appointed at the end of 2003. Congress provided little funding this year to the EAC and none at all to NIST to begin to carry out its duties under HAVA. (At the Science Committee's instigation, the Administration was able to find $350,000 for NIST to carry out some of the most urgently needed work.) As a result, the current testing regime is essentially identical to that which existed before Congress passed HAVA.

The FEC Testing Regime

The standards used today were first issued by the FEC in 1990 and last updated in 2002. Those standards, known as the Voting System Standard (VSS), deal with performance, security, and other aspects of voting systems have existed since 1990. The FEC developed the standards on a limited budget with input from NASED, voting experts, manufacturers, and interest groups, such as the disabled and the League of Women Voters, many of whom participated on a volunteer basis. Although no federal mandate requires that the standards be used, some States have adopted them as mandatory requirements.

To qualify voting machines under the FEC standards, manufacturers must send their equipment to a NASED-approved laboratory (ITA) for testing and inspection. There are three ITAs: Wyle Laboratories, which tests hardware; and CIBER and SysTest laboratories, which test software.

Prior to HAVA, the Federal Government had no official role in approving ITAs. The FEC did cooperate informally with NASED to identify laboratories that could become ITAs. However, few laboratories were willing to participate because they viewed voting machine certification as a risky venture that was unlikely to generate much revenue.

Once a voting machine or its software has passed the current testing process, it is added to the NASED list of "Qualified" voting systems, which means they have met the FEC standards. The only publicly available information is whether a particular machine has passed testing; the complete tests results are not made public because they are considered proprietary information.

Voting technology experts have raised a number of concerns about the standards and testing under the FEC system. They include:

- Some of the FEC Voting System Standards are descriptive rather than quantitative, making it more difficult to measure compliance.
- Many of the FEC Voting System Standards are described very generally, for example those for security. Although this avoids dictating specific technologies to the manufacturers, the standards may require more specificity to be meaningful and effective.
- The ITAs do not necessarily test the same things in the same way so a test for a specific aspect of computer security in one lab may not be the same test used in another.
- Hardware and software laboratories do not necessarily know each other's testing procedures, and although communication takes place between them, they are not required to integrate or coordinate their tests.

- The ITAs, once chosen, are not regularly reviewed for performance. Reaccreditation would help ensure that quality and expertise did not decline or otherwise change over time, and that any new testing protocols were being carried out appropriately.
- Few States effectively test voting machines once they are delivered even though ITA testing—like most product testing—tests samples rather than every unit of a product. When Georgia, in association with Kennesaw State University, conducted their own independent test of their new machines, the State sent five percent of them back to the manufacturer for various defects.
- Companies offer, and States install, last-minute software "patches" that have not been subjected to any testing. California recently decertified new voting machines because they included untested software patches.
- The small number of ITAs limits the amount of competition on the basis of either price or quality.
- As is the case in most product testing, manufacturers, rather than disinterested third parties, pay for the testing.

The Pending NIST Testing Regime

To fully implement HAVA, NIST will have to develop, and the EAC will have to approve standards that the voting equipment must meet (to replace the FEC Voting Systems Standards); tests to determine whether voting equipment complies with those standards; and tests to determine whether laboratories are qualified to become ITAs. NIST has begun preliminary work on some of these tasks, but has been constrained by scarce funds.

Under HAVA, NIST is also to conduct an evaluation of any laboratory that wishes to become an ITA (including ITAs that were already accredited under the NASED system). Accreditation would then be granted by the EAC based on NIST's recommendations. HAVA also requires NIST to monitor the performance of the ITAs, including, if necessary, recommending that the EAC revoke an ITA's accreditation. (These provisions of HAVA originated in the House Science Committee.)

NIST has not yet begun to implement this aspect of HAVA, but NIST recently announced that it will soon convene a meeting for those laboratories that are interested in becoming ITAs to discuss what qualifications they must meet.

Since NIST has just begun developing lab accreditation standards, as an interim measure, NIST will probably accredit laboratories as ITAs using a generic, international standard for laboratories, known as ISO 17025. NIST uses that standard already as part of its existing program for certifying laboratories for other purposes, known as the National Voluntary Laboratory Accreditation Program (NVLAP).

Obviously, none of this will be done in time to affect the purchase of equipment for the 2004 elections, and many States are making large purchases of voting equipment now with the money available under HAVA. However, a number of large States have not yet purchased equipment partly because of uncertainty about what the new standards will be.

Limitations of Laboratory Testing in Reducing Errors in Voting Equipment

An improved federal certification process is a necessary, but not sufficient condition for improving the performance of voting equipment. According to experts, among the issues that remain are:

- No one is required to abide by the new system, although presumably States will want to buy equipment that meets the EAC standards and has been tested in federally certified ITAs.
- Laboratories cannot test every situation that may arise in the actual use of voting machines. Election experts say States should do their own testing, including simulated elections. Some States, for example Georgia, California, and Florida, are implementing tests of their own.
- Pollworker training and voter education are critical to reducing human error and resulting problems with voting equipment. Technology that works perfectly can still be confusing to the users.

WITNESS QUESTIONS

In their letters of invitation, the witnesses were asked to respond to the following questions:

Questions for Dr. Semerjian:

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?
2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006? Do enough Independent Testing Authorities exist to carry out the needed tests? If not, what can be done to increase the number of laboratories?
3. What progress has NIST made in carrying out the requirements of the Help America Vote Act?

Questions for Mr. Wilkey:

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?
2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?
3. Do enough Independent Testing Authorities exist to carry out the needed tests? If not, what can be done to increase the number of laboratories?

Questions for Ms. Coggins:

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?
2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?
3. How do standards affect the way you test voting equipment?

Questions for Dr. Shamos:

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?
2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?
3. How important is NIST's role in improving the way voting equipment is tested? What activities should States be undertaking to ensure voting equipment works properly?

APPENDIX A

Who Tests Voting Machines?

New York Times Editorial
MAY 30, 2004

Whenever questions are raised about the reliability of electronic voting machines, election officials have a ready response: independent testing. There is nothing to worry about, they insist, because the software has been painstakingly reviewed by independent testing authorities to make sure it is accurate and honest, and then certified by State election officials. But this process is riddled with problems, including conflicts of interest and a disturbing lack of transparency. Voters should demand reform, and they should also keep demanding, as a growing number of Americans are, a voter-verified paper record of their vote.

Experts have been warning that electronic voting in its current form cannot be trusted. There is a real danger that elections could be stolen by nefarious computer code, or that accidental errors could change an election's outcome. But State officials invariably say that the machines are tested by federally selected laboratories. The League of Women Voters, in a paper dismissing calls for voter-verified paper trails, puts its faith in "the certification and standards process."

But there is, to begin with, a stunning lack of transparency surrounding this process. Voters have a right to know how voting machine testing is done. Testing companies disagree, routinely denying government officials and the public basic information. Kevin Shelley, the California Secretary of State, could not get two companies testing his State's machines to answer even basic questions. One of them, Wyle Laboratories, refused to tell us anything about how it tests, or about its testers' credentials. "We don't discuss our voting machine work," said Dan Reeder, a Wyle spokesman.

Although they are called independent, these labs are selected and paid by the voting machine companies, not by the government. They can come under enormous pressure to do reviews quickly, and not to find problems, which slow things down and create additional costs. Brian Phillips, president of SysTest Labs, one of three companies that review voting machines, conceded, "There's going to be the risk of a conflict of interest when you are being paid by the vendor that you are qualifying product for."

It is difficult to determine what, precisely, the labs do. To ensure there are no flaws in the software, every line should be scrutinized, but it is hard to believe this is being done for voting software, which can contain more than a million lines. Dr. David Dill, a professor of computer science at Stanford University, calls it "basically an impossible task," and doubts it is occurring. In any case, he says, "there is no technology that can find all of the bugs and malicious things in software."

The testing authorities are currently working off 2002 standards that computer experts say are inadequate. One glaring flaw, notes Rebecca Mercuri, a Harvard-affiliated computer scientist, is that the standards do not require examination of any commercial, off-the-shelf software used in voting machines, even though it can contain flaws that put the integrity of the whole system in doubt. A study of Maryland's voting machines earlier this year found that they used Microsoft software that lacked critical security updates, including one to stop remote attackers from taking over the machine.

If so-called independent testing were as effective as its supporters claim, the certified software should work flawlessly. But there have been disturbing malfunctions. Software that will be used in Miami-Dade County, Fla., this year was found to have a troubling error: when it performed an audit of all of the votes cast, it failed to correctly match voting machines to their corresponding vote totals.

If independent testing were taken seriously, there would be an absolute bar on using untested and uncertified software. But when it is expedient, manufacturers and election officials toss aside the rules without telling the voters. In California, a State audit found that voters in 17 counties cast votes last fall on machines with uncertified software. When Georgia's new voting machines were not working weeks before the 2002 election, uncertified software that was not approved by any laboratory was added to every machine in the state.

The system requires a complete overhaul. The Election Assistance Commission, a newly created federal body, has begun a review, but it has been slow to start, and it is hamstrung by inadequate finances. The commission should move rapidly to require a system that includes:

Truly independent laboratories. Government, not the voting machine companies, must pay for the testing and oversee it.

Transparency. Voters should be told how testing is being done, and the testers' qualifications.

Rigorous standards. These should spell out in detail how software and hardware are to be tested, and fix deficiencies computer experts have found.

Tough penalties for violations. Voting machine companies and election officials who try to pass off uncertified software and hardware as certified should face civil and criminal penalties.

Mandatory backups. Since it is extremely difficult to know that electronic voting machines will be certified and functional on Election Day, election officials should be required to have a non-electronic system available for use.

None of these are substitutes for the best protection of all: a voter-verified paper record, either a printed receipt that voters can see (but not take with them) for touch-screen machines, or the ballot itself for optical scan machines. These create a hard record of people's votes that can be compared to the machine totals to make sure the counts are honest. It is unlikely testing and certification will ever be a complete answer to concerns about electronic voting, but they certainly are not now.

APPENDIX B

The Help America Vote Act (HAVA)

In 2002, the President signed the Help America Vote Act (HAVA) into law, which included a number of measures intended to improve the U.S. election system. Among other things, HAVA banned the use of punch card and lever voting machines and provided funds to the States to replace them. It established an Election Assistance Commission (EAC) to assist in the administration of federal elections and the administration of certain federal election laws and programs, and otherwise oversee the reforms recommended under HAVA. HAVA also established a number of basic requirements that voting machines and systems should meet, and a process by which new voluntary technical standards could be developed to ensure the reliability and accuracy of new voting equipment.

The Science Committee included provisions in HAVA that designated the Director of the National Institute of Standards and Technology (NIST) to chair the Technical Guidelines Development Committee (TGDC), a 14-member panel charged with the development of voluntary voting system guidelines, or standards. HAVA also created a 110-member Standards Board consisting of State and local election officials, and a 37-member Board of Advisors consisting of representatives from various associations, who together would review the standards recommended by the TGDC. The EAC was given the final word on whether these standards would be officially adopted. Once adopted, it would still be up to the States to determine whether the equipment they bought needed to meet the standards, since they are meant to be voluntary, not coercive.

Chairman EHLERS. It is my pleasure to call this hearing to order. It is a hearing on *Testing and Certification for Voting Equipment: How Can the Process be Improved?* And we—I apologize for the delay in starting. That is the bad news. The good news is we are now unlikely to be interrupted by votes for the remainder of the hearing, so we should be able to proceed directly through it.

I am pleased to welcome you today to today's hearing on improving the testing and certification of voting equipment. Most of the national attention on voting systems has focused on the subjects of computer hacking and voter verifiable paper ballots. However, recently, the *New York Times* and other organizations have brought more public attention to the subject of voting machine testing, the laboratories that test the machines, and the development of standards used to conduct the tests.

All new models of voting machines sold in the U.S. today are certified by the National Association of State Elections Directors after having passed a series of tests administered by Independent Testing Authorities, known as ITAs, which are private laboratories. These tests are conducted to ensure that the machines meet certain standards for environmental tolerances, logic, and accuracy, computer security, and other metrics that make them fit for use in elections. Voting machines must also be certified by individual states before they can be purchased by State or local election officials.

However, each election season, a small number of newly deployed voting machines fail to perform properly in the field, causing confusion in the polling places, and concerns over the potential loss of votes. Because these machines have already been tested and certified against Federal Election Commission standards, these incidents have raised questions about the reliability of the testing process, the credibility of standards against which the machines are tested, and the laboratories that carry out the tests. We must resolve this issue soon, because states are already receiving billions of federal dollars under the Help America Vote Act, or HAVA, to modernize their voting systems. It is crucial that voting systems be easy to use, accurate, verifiable, secure, and reliable, and all of those criteria must be met.

The Science Committee, through HAVA, gave the National Institute of Standards and Technology, known as NIST, the role of improving the accreditation process of the laboratories carrying out the tests, and the standards against which machines must be tested and certified. Ultimately, NIST's activities under HAVA will improve the overall quality and performance of voting machines.

Unfortunately, NIST did not receive any funding for these activities for this fiscal year, and the Administration did not request any for 2005. I am working with my colleagues to rectify this situation and provide NIST the money it needs. I am also encouraged that the Election Assistance Commission, which was created in HAVA to oversee overall voting reform, is requesting specific funding in 2005 for these important NIST activities.

I look forward to hearing from our distinguished panel on how best to improve the testing and certification process for voting equipment. And I would like to add that this has been a project dear to my heart ever since the Florida election of a few years ago.

I do have to say that what happened there was absolutely no surprise to me whatsoever. Anyone who has been through the electoral process before knows how easy it is for mistakes to occur, typically using poll workers who do it only a few times a year, and in fact, in my very first election, there was a problem because my opponent's listing and mine were switched in one polling place. I still won, but there was that problem, and it could have swung the election.

The—it is very important for us to ensure the integrity of the voting process, and I must add I am particularly concerned about the possibilities of fraud, even though those of you testifying here today obviously are not the sort of persons who would commit voter fraud, but there is, I believe, an increasing trend of voter fraud across the country. We managed to get rid of Tammany Hall and all the other political machines of the past, where the fraud was quite obvious and deliberate, but I, in my work on the committees dealing with elections in the House, I have discovered that there are increasing problems with fraud in various parts of the country, and so we have to make sure that all our machines are fraud-proof to the greatest extent possible.

Having said that, I would like to turn to the Ranking Member for his opening statement.

[The prepared statement of Chairman Ehlers follows:]

PREPARED STATEMENT OF CHAIRMAN VERNON J. EHLERS

Welcome to today's hearing on how to improve the testing and certification of voting equipment.

Most of the national attention on voting systems has focused on the subjects of computer hacking and voter-verifiable paper ballots. However, recently the *New York Times* and other organizations have brought more public attention to the subject of voting machine testing, the laboratories that test the machines, and the development of standards used to conduct the tests.

All new models of voting machines sold in the U.S. today are certified by the National Association of State Elections Directors, after having passed a series of tests administered by Independent Testing Authorities, which are private laboratories. These tests are conducted to ensure that the machines meet certain standards for environmental tolerances, logic and accuracy, computer security, and other metrics that make them fit for use in elections. Voting machines must also be certified by individual States before they can be purchased by State or local election officials.

However, each election season, a small number of newly-deployed voting machines fail to perform properly in the field, causing confusion in the polling places and concerns over the potential loss of votes. Because these machines have already been tested and certified against Federal Election Commission standards, these incidents have raised questions about the reliability of the testing process, the credibility of standards against which the machines are tested, and the laboratories that carry out the tests. We must resolve this issue soon because States are already receiving billions of federal dollars under the Help America Vote Act (HAVA) to modernize their voting systems. It is crucial that voting systems be easy to use, accurate, verifiable, secure, and reliable.

The Science Committee, through HAVA, gave the National Institute of Standards and Technology (NIST) the role of improving the accreditation process of the laboratories carrying out the tests, and the standards against which machines must be tested and certified. Ultimately, NIST's activities under HAVA will improve the overall quality and performance of voting machines.

Unfortunately, NIST did not receive any funding for these activities for this fiscal year and the Administration did not request any for 2005. I am working with my colleagues to rectify this situation and provide NIST the money it needs. I am also encouraged that the Election Assistance Commission, which was created in HAVA to oversee overall voting reform, is requesting specific funding in 2005 for these important NIST activities.

I look forward to hearing from our distinguished panel on how best to improve the testing and certification process for voting equipment.

Mr. UDALL. Thank you, Mr. Chairman. Along with the Chairman, I want to welcome all of you to this hearing today.

As the Chairman mentioned, we are going to address a very important topic, which is the testing and certification of voting equipment and systems. And although this sounds like a set of dry topics, as the Chairman has mentioned, it is something that we rely upon every day. And I want to provide you the example I rely on, as I think everybody here does, on certification from Underwriters Laboratories, or UL, to tell me that my electric appliances are safe. I may not understand the standard and the test performed by UL, but I do understand that the result is a safe and reliable electric appliance. And that is exactly what we are here to examine today, how to ensure that voters can depend on the voting equipment that they use to be safe and reliable.

This isn't an easy task. As the 2000 election pointed out, this is—was a wakeup call for our country, in that it exposed many problems with our voting equipment. And I should note that I think all of us, or most all of us have forgotten that back in 1988, some 16 years ago, NIST identified problems with punch card ballots, and recommended that they be retired from service. Unfortunately, that advice, that prescient advice, was ignored by the FEC and by State election officials.

Four years after the events in Florida, in the last Presidential election, very little has been done to assure the public of the accuracy and integrity of our voting systems. In fact, with the press coverage of problems with the new generation of voting equipment, I wouldn't be surprised to find the public even more skeptical than they were four years ago. We have mentioned earlier HAVA, H-A-V-A, which passed with great fanfare, on the critical issue of testing and certification. The Administration has never requested the funds for NIST to do its job. And Congress, including this committee, have been lax, I believe, in its responsibilities, by not conducting appropriate oversight of the implementation of HAVA.

My biggest concern at this point is that now we are faced with the sole option of too little, too late. I don't doubt that with time and money, NIST, the head of the Technical Guidelines Development Committee, could develop a rigorous set of standards, testing criteria, and an independent lab testing system. But we are less than four months from the November elections. We can't afford to be complacent and hope that the next election will run smoothly. And I think if there are problems, we may spend years rebuilding the public's confidence in our voting system. We need to squarely face the fact that there have been serious problems with voting equipment deployed across the country in the past two years.

Let me end by reassuring the witnesses that I am not here to find blame. I think the blame, if there is blame to be apportioned, rests squarely with this Administration and this Congress. What I hope to learn today is that we can do some things to assure the public that the voting systems that they use are accurate, reliable, and secure.

So I look forward to the testimony, and I would also add that we are—Mr. Chairman, we have been joined by Carolyn Coggins, who

will sit on the second panel, who is a resident of Colorado, and whose business operations are in the 2nd Congressional District in part. So I want to welcome her in particular. With that, I would yield back if I have any time left.

[The prepared statement of Mr. Udall follows:]

PREPARED STATEMENT OF REPRESENTATIVE MARK UDALL

Good afternoon. I'd like to welcome everyone to today's hearing.

Today we are going to address a very important topic—the testing and certification of voting equipment and systems. Although testing and certification sounds like a dry topic, it is something that we rely upon everyday.

For instance, I rely on certification from Underwriters Laboratories, or UL, to tell me that my electric appliance is safe to use. I may not understand the standard and test performed by UL, but I do understand that the result is a safe and reliable electric appliance. That's exactly what we're here to examine today—how to ensure that voters can depend on the voting equipment they use to be safe and reliable.

This is no easy task. The 2000 election was a wake-up call for this country in that it exposed problems with our voting equipment. I should note that many people have forgotten that back in 1988, NIST identified problems with punch-card ballots and recommended that they be retired from service. Unfortunately, NIST's advice was ignored by the FEC and by state election officials.

So in March 2001, Democratic Members of the Science Committee and I introduced the first bill that called upon NIST to lead a Commission to develop standards and testing procedures for election equipment and systems. This base concept was eventually incorporated into the Help America Vote Act (HAVA), which brings us to today's hearing.

Four years after the last presidential election, very little has been done to assure the public of the accuracy and integrity of our voting systems. In fact, with press coverage of problems with the new generation of voting equipment, I would not be surprised to find the public more skeptical than they were four years ago.

Although HAVA was passed with great fanfare, on the critical issue of testing and certification the Administration has never requested the funds for NIST to begin to do its job. And Congress—including the Science Committee—has been lax in its responsibilities by not conducting appropriate oversight of the implementation of HAVA.

My biggest concern is that we are now faced with the sole option of "too little, too late." I don't doubt that with time and money, NIST—as the head of the Technical Guidelines Development Committee (TGDC)—could develop a rigorous set of standards, testing criteria, and an independent lab testing system.

But we are less than four months from the November elections. We can't afford to be complacent and hope that the next election will run smoothly. If there are any problems, we will spend years rebuilding the public's confidence in our voting systems. We need to squarely face the fact that there have been serious problems with voting equipment deployed across the country in the past two years.

I want to reassure the witnesses that I'm not here to find blame—the blame rests squarely with this Administration and the Congress. What I hope to learn today is what can be done to assure the public that the voting systems they use are accurate, reliable and secure.

I look forward to your testimony.

Panel I

Chairman EHLERS. I thank the gentleman for yielding back. We will begin with the first panel, consisting of one person, and at this time, I am pleased to introduce my colleague from New Jersey, my fellow physicist, Representative Rush Holt, who will provide his comments on this important topic.

As both Rush and I know, physicists are both omniscient and omni-competent, and so I am looking forward to hearing his testimony.

Mr. Holt.

STATEMENT OF HON. RUSH HOLT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. HOLT. Thank you, Mr. Ehlers, Mr. Udall, Mr. Burgess, Mr. Gutknecht, Mr. Baird, Mr. Matheson. Thank you for having me here today. I have some prepared testimony that I would like to leave with you, but let me give a few summary remarks, if I may.

We should begin by noting that it was the advent in the use of computers in voting that precipitated the development of national standards in the voting systems. The 2001 Caltech MIT Voting Technology Project reported that the first national effort to develop standards, a joint project of the then Bureau of Standards and the General Accounting Office Office of Federal Elections, focused on the accuracy and security of computerized voting systems. That was more than 25 years ago.

Now, in the wake of 2002 elections, despite the enactment of the Help America Vote Act, what are we experiencing? Well, one after another, incidents or irregularities reported, on various computer voting systems. 100,000 votes disappearing into cyberspace, or maybe 100. Xes jumping from one candidates name to another. You know, 100,000 votes being recorded in a district where only 19,000 are registered to vote, and only 5,000 turned up that day at the polls. In one jurisdiction after another election officials are being given pause.

Now, like you, Mr. Ehlers, I am not surprised about this. As a physicist, I have programmed computers. I understand the kinds of things that could go wrong, and I am sure you and I, or any of us, could swap election stories of apparent irregularities, or close calls, or recounts, or whatever. What it comes down to today, a fundamental fact, that with the computer voting devices today, there is a gap between the casting of the vote and the recording of the vote that makes the process quite a bit different than what we have been used to before.

When voting machines were simple, mechanical devices, no one much cared if the manufacturers helped local officials select and maintain their equipment, but with more sophisticated, computerized machines, and the sudden availability of hundreds of millions of dollars in federal subsidies, it has raised questions in the minds of members of the public and election officials.

You know, in November 2003, allegations surfaced to the effect that uncertified software had been used in electronic voting systems in at least two California counties. In response to these allegations, the Secretary of State of California ordered an independent review be conducted of all voting systems in the state, and he has subsequently imposed a number of requirements on future voting in the state, particularly with regard to electronic or computerized voting machines.

The Caltech MIT Voting Technology Project, to which I referred earlier, said that, quote, existing standards—the existing standards process is a step in the right direction, but it does not cover many of the problems that we have detected, the project has detected. Important things are not reviewed currently, including ballot and user interface designs, auditability, and accessibility. Well, HAVA went a long way in improving accessibility, and despite a certain amount of, well, some mention of auditability, I think it failed to

really deal with that question, and it is on that that I wanted to spend a couple of minutes, because I think it has important implications for the certification process.

With the computers, the mechanism is not transparent. Any of us who has programmed computers or has tried to debug someone else's program knows how easy it is for an error to lie undetected. A bug can enter the system in various ways, inadvertently or by malicious hacking. With the difficulty of monitoring all machines at all times, and the ease with which changes could be made, the ease with which changes could be concealed, or as I say, escape detection, it means that there is a much higher burden, and it is not good enough to just certify a certain machine, or even a certain class of machines. What is possible is that these problems could go undetected, and what concerns me even more than all of these reported irregularities that we have read about in the papers are the ones that have gone undetected, that we will never know about, that will not be subject to a recount because the margin maybe wasn't so small. There could be errors that we would never know about, and therefore, the certification process, I think, has to be designed to get at that, and the only way, I believe, that we can get at that problem is through auditability. In other words, a verifiability that is built into the system, and that is part of the audit process.

I commend the Committee for holding these hearings, and I think it is important that we ensure that the testing and certification procedures used to scrutinize and safeguard the equipment have the highest possible caliber, but it is different from auditing other machines. It is different from auditing ATM or bank machines, because it is a secret ballot, and each ballot is secret, and therefore, it is impossible for the manufacturer and the vendor, or any election official, to reconstruct the intention of the voter in that secret booth. Only the voter knows his or her intention, and only the voter is in a position to verify whether the vote is recorded the way that she or he intended. That is why it is important that a process be built in to the system for verification, and I would argue that verification must belong to the voter, and I think the implications for certification are what should be explored in that context.

[The prepared statement of Mr. Holt follows:]

PREPARED STATEMENT OF REPRESENTATIVE RUSH HOLT

Distinguished Members of the Committee, thank you for inviting me to come before you today to address the matter of the testing and certification of voting systems used in the United States, as well as the accreditation of independent testing authorities (ITAs). As the Committee knows, the integrity of the electoral system in the United States is a matter of great concern to me. Any and all current shortcomings in existing testing, certification and accreditation procedures must certainly be addressed, but in addition, the inherent limits in the protection that may be provided by even the best such procedures must also be acknowledged.

It should be noted that it was the advent of the use of computers in voting that precipitated the development of national standards for voting systems. Prior to the use of computers in the electoral system, there were no national standards for voting systems, nor, I expect, did anyone particularly see the need for them. When voting systems were strictly paper-based, or strictly mechanical, the average citizen—or election official—could readily understand all there was to know about the system, and implement it without extensive study or training. With the advent of computer voting systems, the average citizen—and the average election official—has become almost completely reliant on the representations of the system vendors, and the technologists who test and certify them, that the systems will function properly.

The 2001 *Caltech MIT Voting Technology Project* reported that the first national effort to develop standards, a joint project of the National Bureau of Standards and the General Accounting Office's Office of Federal Elections, "focused on the accuracy and security of computerized voting systems." Published in 1975, more than 25 years ago, the report, entitled *"Effective Use of Computing Technology in Vote Tallying"* stated that "one of the basic problems with this technology was the lack of evaluative standards and testing procedures for election systems." That 1975 report led to Congressional action, which resulted in the development of voluntary voting system standards by the Federal Election Commission (FEC) and the National Institute of Standards and Technology (NIST) in 1984, which were used by the FEC to promulgate national standards and testing procedures in 1990. Those 1990 voluntary standards covered punch card, optical scan, and direct recording electronic (DRE) voting systems, and have been adopted by more than half of the states for use in certifying the voting systems used in those states.

The *Caltech MIT Voting Technology Project* continued, however, by saying that "[t] existing standards process is a step in the right direction, but it does not cover many of the problems that we have detected. . .important things are not reviewed currently, including ballot and user interface designs, auditability, and accessibility." Auditability is, and obviously must be, among the very most critical aspects of any testing and certification process. The *Caltech MIT* study further stated, under the heading "Create a New Standard for Redundant Recordings," "[a]ll voting systems should implement multiple technological means of recording votes. For example, DRE/touchscreen systems should also produce optical scan ballots. This redundancy insures that independent audit trails exist post-election, and it helps insure that if fraud or errors are detected in one technology there exists an independent way to count the vote without running another election."

The *Caltech MIT* study reported the results of a 12-year study covering elections between 1988 and 2000. It was the joint effort of computer scientists, human factors engineers, mechanical engineers and social scientists; the project organizers met with leading election officials, researchers and industry representatives. In their joint statement releasing the report, the Presidents of the California Institute of Technology and the Massachusetts Institute of Technology said that in the aftermath of the 2000 election "America learned that at the heart of their democratic process, their 'can-do' spirit has 'make-do' technology as its central element. For many years, we have 'made do' with this deeply flawed system, but we now know how poorly these systems function. Until every effort has been made to insure that each vote will be counted, we will have legitimate concerns about embarking on another presidential election."

In the wake of the 2000 election, hundreds, if not thousands, of the best minds in our country were working on the problem of our flawed election system. The 2001 *Caltech MIT* study was released well before the Help America Vote Act (HAVA) was passed in October 2002. And yet, HAVA did not mandate what this critical study recommended—standards, if not actual laws—requiring an independent audit mechanism. Not a privatized audit mechanism, not a vendor-verified audit mechanism, but a meaningful, independent audit mechanism.

In the wake of the 2002 election, and despite the enactment of HAVA, what are we experiencing? One after another incident of irregularities reported on computer voting systems. 100,000 votes disappearing into cyberspace, or even just 100. "X"s jumping from one candidate's name to another. More than 100,000 votes being recorded in a district where only 19,000 were registered to vote, and only 5,000 voted. In one jurisdiction after another, election officials are being given pause.

Despite the fact that national standards have been developed and implemented and improved upon over the past three decades, and despite the fact the standards in use today do cover and have been used to certify DRE and other electronic voting systems, electronic voting system irregularities have not been prevented. Let's consider the example of California.

In November 2003, allegations surfaced to the effect that uncertified software had been used in electronic voting systems in at least two California counties. In response to those allegations, Secretary of State Kevin Shelley ordered that an independent audit be conducted of all voting systems used in the state. In his press release announcing the audit he said "[T]o ensure that the integrity of California's elections process has not been compromised, I will make certain that all California systems are in compliance with State security standards." The result of the audit—it was discovered that Diebold Election Systems had used uncertified software in all 17 California counties in which it's electronic voting equipment was used. Fourteen of those counties had used software that had been federally qualified, but not certified by State authorities. The other three used software that had not been certified at the State nor qualified at the federal level. In April 2004, Secretary of State

Shelley banned the use of touch screen systems in four counties and decertified all touch screen systems in California for use unless and until those systems were brought into compliance with additional security measures. Kevin Shelley's Decertification Order, and his recently release standards for Accessible Voter Verified Paper Audit Trail Systems, are attached as Appendix A.

California is in a sense an extreme example, but perhaps only because Secretary of State Shelley acted upon the first indication of a problem, and discovered and confronted those problems. But again, reports of irregularities on electronic voting systems abound, and have occurred in states from one shore of this country to the other. In how many other states might similar deficiencies in testing or certification be found? As we all know, the voting systems Secretary of State Shelley decertified in 2004 had just been used in the recall election in California in 2003. And those touch screen systems were not independently unauditable. Three decades of work developing and fine tuning national standards did not protect voters in the State of California, and have not necessarily protected voters elsewhere. Were those three decades of effort all for naught? Of course not. Were the standards developed worthless? Of course not. But we can plainly see by this one example that perfecting testing and certification procedures is not, nor will it ever be, the end of the inquiry.

Johns Hopkins Computer Scientist Aviel Rubin, co-author of the analysis released in the summer of 2003 that described "stunning, stunning" flaws in the software used in Maryland's touch screen voting systems, has issued a challenge, entitled *"Can a Voting Machine that is Rigged for a Particular Candidate Pass Certification?"* In it he says "[p]roponents of DREs argue that the ITA [Independent Testing Authorities] process would catch any attempts to manipulate the results. They argue that Trojan horse programs would have to have magical properties and that they would be detected. They further argue that techniques such as parallel testing, where machines are selected at random and elections are run on them on election day where they are checked for accuracy, ensure that no such rigging is possible. Security experts do not buy these arguments."

In short, Professor Rubin proposes that a team of computer security experts be given access to one of the major vendors, full authority to produce a rigged machine, and that that machine then be presented to an ITAs that is unaware of the challenge, along with all the other machines, to determine whether the ITA could discover the rigging. If not, that would demonstrate that voting system vendor's employee could rig an election. Would any of the ITAs accept this challenge? Would any vendor? I think it would be a worthwhile endeavor, although, as Professor Rubin points out, the testing and certification process is analogous to airline security procedures—"just like successfully catching an agent with a concealed weapon at the airport does not mean the next guy won't get through," even if the ITA in question discovers the rigged machine in question, that doesn't mean the next rigged machine won't get through.

Even in the absence of such a challenge, the Committee should leave no stone unturned in determining exactly how the Diebold systems used in California, Maryland other jurisdictions have passed muster with the ITA's in question. In every instance in which an irregularity has been reported in connection with the use of any electronic voting system, the same inquiry should be made. In every instance, the Committee should ask, are testing and certification procedures capable of being implemented with perfection? Will they find every flawed or rigged machine? In the wake of September 11, despite the obviously heightened security at our airports, has every single weapon sought to be smuggled onto an aircraft, has every mechanical malfunction, been found before take-off?

It is also of critical importance to note that the "revolving door" for employees between vendors, testers and certifiers perhaps ought to be closed, permanently. Going back to California, take for example the recent report in the San Francisco area online periodical the *Contra Costa Times:*

> "Critics say. . .close, often invisible, bonds link election officials to the equipment companies they are supposed to regulate. When voting machines were simple mechanical devices, no one much cared if manufacturers helped local officials select and maintain their equipment. But a switch to sophisticated computerized machines, and the sudden availability of hundreds of millions of dollars in federal subsidies, has raised questions about counties' dependence on private firms. While a revolving door between government service and private-sector jobs is common, some observers argue that such cozy familiarity has led public officials to overlook flaws in controversial electronic voting systems, putting elections at risk."

Attached as Appendix B to my statement is a copy of an editorial published in the *New York Times* on June 13, 2004, entitled *"Gambling on Voting,"* which makes

the point that slot machines are subject to more rigorous testing and certification procedures than voting systems.

I would like to commend the Committee for holding this hearing, and for taking action to ensure that the testing and certification procedures used to scrutinize and safeguard the equipment used in our elections are of the highest possible caliber. But I would at the same time urge the Committee to recommend, as was recommended by the *Caltech MIT* study, that DRE/touch screen systems produce optical scan or other paper ballots, so that an independent audit trail will exist in each election, and help insure that if fraud or errors are detected there will be an independent way to count the vote short of running another election. We most definitely "can-do" this, and "making-do" without it does nothing short of placing this very democracy at risk.

State of California

SECRETARY OF STATE

DECERTIFICATION AND WITHDRAWAL OF APPROVAL OF CERTAIN DRE VOTING SYSTEMS AND CONDITIONAL APPROVAL OF THE USE OF CERTAIN DRE VOTING SYSTEMS

I. Recitals

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State;

Whereas, existing law requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable for use;

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, to determine if they are defective, obsolete, or otherwise unacceptable for use in the November 2004 General Election in California;

Whereas, on April 21, 2004, April 22, 2004, and April 28, 2004, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the use of various voting systems in the November 2004 General Election in California. At these hearings approximately 100 individuals testified. Many more submitted comments by letter, fax and electronic mail;

Whereas, following the duly noticed public hearing on April 21, 2004, April 22, 2004, and April 28, 2004, the Voting Systems and Procedures Panel recommended that I withdraw approval of the use of certain voting systems to be used at the November 2004 General Election unless certain conditions for their use were implemented;

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State am authorized to withdraw approval previously granted of any voting system or part of a voting system should I determine that voting system or any part of that voting system be defective or otherwise unacceptable;

Whereas, I have reviewed voting systems approved for use in California and I have reviewed and considered several reports regarding the use of voting systems, including Direct Recording Electronic (DRE) voting systems and other voting systems, the public testimony presented at the hearings referenced above, numerous communications from elections officials, State Legislators, members of the disabled community, voting rights advocates, vendors of voting systems and interested members of the public, and other materials, as well as the findings and recommendations of the Voting Systems and Procedures Panel;

Whereas, pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting system unless I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary;

Whereas, pursuant to Elections Code section 19222, any withdrawal of approval by the Secretary of State of previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal;

II. *Therefore*, I, Kevin Shelley, Secretary of State for the State of California, find, determine and order, pursuant to Division 19 of the Elections Code and Government Code section 12172.5, as follows:

A. Findings and Determinations

1. DRE voting systems currently approved for use in California pursuant to Division 19, Chapter 1 (commencing with Section 19001) of the Elections Code and Government Code section 12172.5:

    a. Do not produce an accessible voter verified paper audit trail permitting a voter to independently and contemporaneously verify the accuracy of the electronic vote recording so as to ensure that his or her vote is counted in accordance with Section 2.5 of Article II of the *California Constitution*;

b. Do not permit meaningful recounts specified in Elections Code sections 15360, 15610, 15620, 15621, 15623, 15627 and 15640;

c. May not permit a contest to be decided by a meaningful recount of the votes, as provided for in Division 16 (commencing with section 16000) of the Elections Code;

d. Use proprietary source codes that are complex and secret so that the absence of malicious code in the firmware is extremely difficult, if not impossible, to prove or determine;

e. Involve sophisticated electronic technology that cannot easily be operated and, when necessary, repaired by many poll workers, which sometimes results in voters not voting the correct ballot type and which is sometimes vulnerable to unexpected functional failure resulting in the disenfranchisement of voters;

f. May be the subject of erroneous programming or other human errors that may not be detected prior to the commencement of voting;

g. May be subject to tampering and/or manipulation if insufficient security enhancements are not in place or are not properly implemented;

B. Orders

***Therefore*, I, Kevin Shelley, Secretary of State for the State of California, hereby direct, pursuant to Division 19, Chapter 1 (commencing with Section 19001) of the Elections Code and Government Code section 12172.5, that:**

1. For the reasons set forth above, DRE voting systems, including but not limited to the Diebold AccuVote-TS, the ES&S iVotronic, the Sequoia AVC Edge, and the Hart eSlate, and any other DRE voting system, previously approved, are found and are determined to be defective or unacceptable and approval for their use in subsequent elections in California is immediately decertified and withdrawn, except as specifically provided below.

2. DRE voting systems are approved for use in California only if (a) Paragraph 3 **or** 4 below applies **and** (b) Paragraph 5 below applies.

3. No new DRE voting system may be used in California unless it includes a fully tested, federally qualified and state certified accessible, voter verified, paper audit trail, and there is compliance with all of the conditions set forth in Paragraph 5 below. For purposes of this paragraph, any modified version of the Diebold AccuVote-TSx voting system submitted to the Secretary of State for certification shall be deemed to be a new DRE voting system.

4. DRE voting systems used in the March 2, 2004 Statewide Primary Election, but not including the AccuVote-TSx voting system, are approved for use in the jurisdictions in which they were previously used if there is compliance with all of the conditions set forth in Paragraph 5 below. In addition, such voting systems, as a condition of approval of their use in subsequent elections, must comply with the following conditions:

    a. The voting system must include a fully tested, federally qualified and state certified accessible, voter verified paper, audit trail; **or**

    b. There must be compliance with the following conditions:

        (1) Permit every voter to have the option at his or her polling place of casting a ballot on a paper ballot which may be satisfied by providing an adequate number of paper ballots to each polling place based on each County's assessment of the number of persons who may request them. The cost of additional paper ballots specified in this paragraph shall be borne by the vendor of the voting system that sought its certification or approval for use in California, or the vendor's successor in interest;

        (2) At the time the ballot is cast or during the period allowed for conducting the official canvass, a paper version or representation of each ballot cast on each unit of the voting system shall be printed out on paper. The paper version shall not be provided to the voter but shall be retained by elections officials for use during the one percent manual recount or other recount or contest. The cost of printing a paper version or representation of each ballot cast on each unit and the storage

of such printouts specified in this paragraph shall be borne by the vendor of the voting system that sought its certification or approval for use in California, or the vendor's successor in interest;

(3) The voting system shall be subject to "parallel monitoring" as directed by the Secretary of State;

(4) At least 46 days prior to any election in which the voting system is proposed to be used, the elections official conducting the election shall submit a Technical Security Plan that is consistent with the directives of the Secretary of State and the recommendations contained in the *Trusted Agent Report to the Maryland Department of Legislative Services by RABA Innovative Solution Cell (RiSC)* dated January 20, 2004 (RABA Report) (http://www.raba.com/press.html?id=9) to the extent that the recommendations are applicable to the voting system proposed for use;

5. All DRE voting systems used in California, including those that include an accessible, voter verified paper audit trail, as defined by the Secretary of State, must meet the following conditions:

a. Certification and Testing

(1) Federal Testing and Qualification The voting system, and all of its hardware, software, and firmware, including all of its peripheral equipment, has been fully tested by and qualified for use by the appropriate federal entities, if applicable;

(2) State Testing and Certification The voting system, and all of its hardware, software, and firmware, including all of its peripheral equipment, has been approved for use in California elections by the Secretary of State of the State of California following full testing;

(3) Documentation

(a) The Source Code for any software and firmware used as part of any of the voting system, including commercial off the shelf software that is available to and disclosable

by the vendor, shall, upon demand of the Secretary of State, at any time before or after approval is requested, be provided to the designee or designees of the Secretary of State for analysis, subject to any reasonable time and confidentiality restrictions, as determined by the Secretary of State;

(b) The full record of all documents submitted or resulting from the federal qualification process shall, upon demand of the Secretary of State, at any time before or after approval is requested, be provided to the designee or designees of the Secretary of State for analysis, subject to any reasonable time and confidentiality restrictions, as determined by the Secretary of State;

(c) Complete documentation of each hardware, software and firmware version for any component of the voting system, including detailed change logs, for any part of the voting system, shall, upon demand of the Secretary of State, at any time before or after approval is requested, be provided to the designee or designees of the Secretary of State for analysis, subject to any reasonable time and confidentiality restrictions, as determined in the sole discretion of the Secretary of State;

(d) Complete documentation regarding the development environment and development process for any software or firmware used in any component of the voting system, including but not limited to configuration files, translators, libraries, and options sufficient to allow exact reconstruction of the object code used in any component of the voting system, shall, upon demand of the Secretary of State, at any time before or after approval is requested, be provided to the designee or designees of the Secretary of State for analysis, subject to any reasonable time and confidentiality restrictions, as determined by the Secretary of State;

(4) Functional Systems Provided to Secretary of State Upon demand of the Secretary of State, at any time before or after approval is requested, the vendor seeking approval or whose

voting system has been approved, shall provide to the Secretary of State, a working version of the components, including all hardware, software and firmware, of the voting system that is proposed to be used at an election, for purposes of analysis and testing, staff reference and public education. The components shall be maintained in working order by the vendor;

(5) Limits on Requests for Late Modifications A request for a change or modification of the voting system that might impair the accuracy and efficiency of the voting system shall not be submitted to the Secretary of State, unless specifically authorized by the Secretary of State, within 46 days prior to any election in which the voting system is proposed to be used.

b. Security

(1) Telephone Connections No component of the voting system shall be permitted to receive official elections results through an exterior communication network, including the public telephone system;

(2) No Wireless Connection Hardware No component of the voting system shall include the hardware necessary to permit wireless communications or wireless data transfers to be transmitted or received;

(3) No Internet Connections No component of the voting system shall be physically connected at any time, directly or indirectly, to the Internet;

(4) Physical Security Plans At least 90 days prior to any election in which the voting system is proposed to be used, the elections official conducting the election shall submit to the Secretary of State, a Physical Security Plan regarding all of the components of the voting system, including the details of how a chain of custody with respect to all of the components is monitored and documented;

(5) Compliance with Directives The elections officials conducting an election using the voting system, and the vendor of the voting system that has sought its certification or approval for use in Califor-

nia, or the vendor's successor in interest, shall abide by any directive issued by the Secretary of State of California, in writing, that is designed to safeguard or enhance the security of the voting system and its use, including, but not limited to, directives related to random audits, poll monitoring, parallel monitoring, security plans, election observer plans, Logic and Accuracy Tests, the providing of tabulation software for escrow with the Secretary of State, and physical security plans. Any such directive will be issued within a reasonable timeframe before the election to allow for full compliance;

c. Poll Workers

(1) Training The elections official conducting the election shall, at least 46 days prior to the election in which the voting system is proposed to be used, submit to the Secretary of State the Poll Worker Training Plan for the election in every jurisdiction using that system, including a copy of the materials to be provided to the poll workers. The training must provide adequate, hands-on training for each poll worker for the voting system being used, including instruction on the use of each component part and the steps to follow if any component of the voting system fails or appears to fail to function properly;

(2) Communication Plan The elections official conducting the election shall, at least 46 days prior to the election in which the voting system is proposed to be used, submit to the Secretary of State a Communications Plan detailing how elections officials and polls workers at each polling place will communicate on Election Day.

d. Polling Places

(1) Provisional Ballots Provisional voters must cast ballots on paper ballots;

(2) Disability Access Devices Disability Access Devices, intended to benefit voters who desire to use such devices, shall be connected to voting machines prior to the time the polls open;

(3) Posting of Results A copy of the results from each voting unit that is capable of printing out a tabulation of the results shall be

posted for public inspection for at least 48 hours outside each polling place;

(4) Tampering Penalties Posted There shall be posted at polling places, in all applicable languages, a notice regarding the penalties for tampering with any component of the voting system;

III. *Therefore*, I, Kevin Shelley, Secretary of State of California, further find and determine, pursuant to Elections Code section 19222, that based on the materials, testimony and comments I have reviewed and considered, and the findings and recommendation of the Voting Systems and Procedures Panel, there is good cause why notice of the withdrawal of approval of voting systems, as specified above, is necessary to be shorter than six months. I also find and determine that it is necessary that such notice be effective immediately in order to provide time for conducting subsequent elections in California fairly, efficiently and to ensure the integrity of the elections process.

It is so found, determined and ordered.

IN WITNESS WHEREOF, I execute this Certificate and affix the Great Seal of the State of California this 30th day of April, 2004.

KEVIN SHELLEY
Secretary of State

June 15, 2004

State of California
Standards For
Accessible Voter Verified Paper Audit Trail Systems
In Direct Recording Electronic (DRE) Voting Systems

These standards have been adopted by the Secretary of State pursuant to Elections Code sections 19100 and 19205 and shall regulate and govern the use of the Accessible Voter Verified Paper Audit Trail System in Direct Recording Electronic (DRE) Voting Systems in all elections governed by the California Elections Code. These standards shall only apply to DRE systems for which an electronic record of the vote is created by the DRE and for which that electronic record is considered the official record.

These standards shall be effective on the date of their adoption for all DRE voting systems purchased after that date and beginning July 1, 2006 for all DRE voting systems, and shall be used in conjunction with all other statutory and regulatory requirements at the state and federal level. Insofar as feasible, all standards prescribed herein shall be carried out in full view f the public.

These standards constitute a minimum standard of performance. They are not intended to preclude additional steps taken by individual elections officials to enhance the security and reliability of the electoral process.

1. General Description

1.1 Components: The accessible voter verified paper audit trail (AVVPAT) system shall minimally consist of:

1.1.1 An Accessible Voter Verified Paper Audit Trail Writer (AVVPAT-W): A device attached, built into, or used in conjunction with a Direct Recording Electronic (DRE) unit. Such a device must minimally consists of:

1.1.1.1 Printer: A device that will duplicate a voter's selections on the DRE onto a paper record copy.

1.1.1.2 A Paper Record Display Unit: A unit that will allow a voter to view his or her paper record copy while preventing the voter from directly handling the paper record copy.

1.1.2 An Accessible Voter Verified Paper Audit Trail Record Storage Unit (AVVPAT-S): A device that stores cast and spoiled paper record copies.

1.1.3 These devices may be integrated as appropriate to their operation.

1.2 Operation: AVVPAT systems may be designed in various configurations. In all such devices, upon completion of selecting his or her contest choices on the DRE, the voter shall have the ability to verify his or her selections on a paper record copy. During the verification, the voter shall either accept or reject the choices represented on the paper record copy. Upon the completion of the verification process, both the electronic record and the paper record copy shall be stored and retained.

2. Design Requirements

2.1 General

2.1.1 Use of Electronic and Paper Records

2.1.1.1 Every electronic record must have a corresponding paper record copy.

2.1.1.1.1 The paper record copy must be printed and the voter must have the opportunity to verify that record prior to the electronic record being recorded.

2.1.1.2 The electronic record shall be considered the official record except as described in 2.1.1.3 and 2.1.1.4.

2.1.1.3 The paper record copy shall be considered the official paper audit record and shall be used for the required 1% manual recount and for any full manual recount.

2.1.1.4 In the case of a difference between the electronic record and the paper record copy, the paper record copy shall govern, unless there is clear evidence that the paper record copy is inaccurate, incomplete or unreadable as defined in the system procedures.

2.1.2 Privacy: The AVVPAT system shall be designed to allow every voter to review, accept or reject his/her paper record copy privately and independently and shall comply with federal and state privacy requirements.

2.1.3 Secrecy: The AVVPAT system shall be designed to ensure secrecy of votes so that it is not possible to determine which voter cast which paper record copy and shall comply with federal and state secrecy requirements.

2.1.4 Readability: The AVVPAT system shall be designed to maximize the ease in which the voter may review, accept or reject his/her paper record copy and shall comply with federal and state readability requirements.

2.1.5 Accessibility: The AVVPAT system shall be designed to allow access for disabled and limited literacy voters to privately and independently use the AVVPAT and shall comply with federal and state accessibility requirements.

2.1.6 Language Accessibility: The AVVPAT system shall be designed to allow each voter to verify their vote on a paper record copy in the same language they voted in on the DRE and shall comply with federal and state requirements.

2.1.7 Security: The AVVPAT system shall be designed to prevent tampering with either the AVVPAT system or the paper record copy, and shall comply with federal and state security requirements.

2.2 Paper Record Copy

2.2.1 Security: Security protections shall be built into the paper record copy and/or AVVPAT-S to prevent tampering. This provision shall apply to paper record copies before, during and after printing.

2.2.2 Readability: The paper shall be designed so as to make the paper record copy readable by voters and election officials and shall comply with federal and state readability requirements.

2.2.3 Capacity: For each statewide election, the elections official shall provide a sufficient number of paper record copies in each precinct to reasonably meet the needs of the voters in that precinct. The same standards shall apply to paper record copies as for paper ballots as defined under federal and state requirements.

2.2.4 Retention: The voter verified paper record copy shall be retained by the elections official for the same period of time as mandated by state and federal law for the retention of paper ballots for that election.

2.3 Printer

2.3.1 Security: The printer shall be physically secure from tampering. The paper record copy and the image created by the AVVPAT-W on the paper record copy shall be designed to withstand storage requirements as outlined in these standards and federal and state requirements.

2.3.2 Readability: The image created by the printer shall be designed to allow a voter to review his or her paper record copy privately and independently.

2.3.3 Printed Information

2.3.3.1 Offices/Measures: The image created by the AVVPAT-W shall include every contest that is displayed to the voter on the DRE review screen.

2.3.3.2 Selections

2.3.3.2.1 Candidates/Measures: The image created by the AVVPAT-W shall include every valid selection made for each contest as selected by the voter.

2.3.3.2.2 Write-in: The image created by the AVVPAT-W shall allow for write-in candidates as mandated by state law.

2.3.3.2.3 Undervote: The image created by the AVVPAT-W shall provide information on the contests for which the voter has not made a selection. This shall not replace the requirement that the DRE notify the voter on the DRE in the case of any undervote.

2.3.3.3 Provisional Ballot: The image created by the AVVPAT-W shall be clearly identifiable in the case of a provisional ballot.

2.3.3.4 Spoiled Ballot

2.3.3.4.1 The image created by the AVVPAT-W shall be clearly identifiable in the case of a spoiled paper record copy. The clearly identifiable spoiled paper record copy shall be shown in the paper record display unit to allow the voter to acknowledge the paper record copy has been spoiled. The AVVPAT system shall be designed to prevent a paper record copy from being spoiled after the voter has verified that paper record copy.

2.3.3.4.2 The voter shall have the opportunity to affirmatively spoil their paper record copy no more than two times. An error in recording or printing a paper record copy not caused by the voter shall not be counted as a spoiled paper record copy.

2.3.3.4.3 Upon spoiling their paper record copy the voter shall be able to modify and verify selections on the DRE without having to reselect all of their choices.

2.3.3.4.4 Before the voter causes a third and final paper record copy to be printed, the voter shall be presented with a warning notice that the selections made on screen will be final and the voter will see and verify a printout of their vote, but will not be given additional opportunities to change their vote.

2.3.4 Language Accessibility

2.3.4.1 The AVVPAT-W shall be capable of producing an image in all alternative languages for which the DRE is certified.

2.3.4.2 The paper record copy shall be printed in English and in the language the voter used to cast their vote on the DRE.

2.4 Paper Record Display Unit

2.4.1 Security: The paper record display unit shall allow the voter to inspect the paper record copy without physically handling the paper record copy and shall be physically secure from tampering.

2.4.2 Readability: The paper record display unit shall provide adequate visual space to allow the voter to privately and independently inspect the paper record copy. A paper record copy shall be readable from the same position and posture used for voting on the DRE. The voter shall have the ability to view both the review screen on the DRE and the paper record copy in the display unit simultaneously. If the paper record copy cannot be viewed in its entirety in the paper record display unit at one time, then the voter shall have the opportunity to verify the entire paper record copy prior to either the electronic record or the paper record copy being stored and recorded.

2.4.2.1 Covering: Any protective covering intended to be transparent shall be in such condition that it can be made transparent by ordinary cleaning of its exposed surface.

2.4.3 Accessibility: The AVVPAT components must conform to federal and state accessibility requirements.

2.4.3.1 This shall include, but is not limited to, an audio component.

2.4.3.1.1 The audio component must accurately relay the information printed on the paper record copy to the voter.

2.4.3.1.2 The data relayed to the audio device must come either directly from the data sent to the printer or directly from the paper record copy.

2.5 Paper Record Storage Unit

2.5.1 Security: The Paper Record Storage Unit shall be designed to prevent tampering.

2.5.2 Secrecy: The AVVPAT system shall be designed to ensure secrecy of votes so that it is not possible to determine which voter cast which paper record copy.

2.5.3 Capacity: The combined capacity of all the paper record storage units in a precinct must be enough to accommodate all voters using the DREs within the precinct.

3. Procedure Requirements

3.1 Update: Testing and pre-election, election and post-election procedures for each DRE voting system shall be updated to reflect the use of the AVVPAT. These updates include, but are not limited to:

3.1.1 Testing and Certification

3.1.1.1 Testing: The AVVPAT system shall conform to federal and state testing requirements. Required testing shall include, but not be limited to, functionality, security, durability, longevity and accessibility testing.

3.1.1.2 Certification: The AVVPAT system must be certified for use by the State of California in conjunction with the rest of the voting system with which it is intended to be used.

3.1.2 Pre-election Procedures: The AVVPAT system components must be integrated into existing local logic and accuracy testing requirements.

3.1.3 Election Procedures

3.1.3.1 Malfunctions

3.1.3.1.1 The vendor shall provide procedures for how to investigate and resolve malfunctions including, but not limited to, misreporting votes, unreadable paper records, paper jams, low-ink, misfeeds and power failures.

3.1.3.1.2 The vendor shall include procedures for how to recover votes in the case of malfunction to assure a ballot is properly recorded and stored.

3.1.3.1.3 The vendor shall include procedures to prevent the AVVPAT system from being a single point of failure within a precinct.

3.1.3.2 The vendor shall include procedures for if the voter does not complete the verification process for their paper record copy.

3.1.4 Post Election Procedures

3.1.4.1 Procedures shall reflect the use of the paper record copies in the required 1% manual recount and any full manual recount.

3.1.4.2 The vendor shall include procedures for how the secrecy of votes will be ensured.

3.1.4.3 The vendor shall include procedures for how a discrepancy between an electronic record and its corresponding paper record copy shall be identified, investigated and resolved.

3.1.4.3.1 The vendor shall include procedures for determining what constitutes clear evidence that a paper record copy is inaccurate, incomplete or unreadable.

Appendix B

Gambling on Voting

PUBLISHED IN THE *New York Times,* June 13, 2004

If election officials want to convince voters that electronic voting can be trusted, they should be willing to make it at least as secure as slot machines. To appreciate how poor the oversight on voting systems is, it's useful to look at the way Nevada systematically ensures that electronic gambling machines in Las Vegas operate honestly and accurately. Electronic voting, by comparison, is rife with lax procedures, security risks and conflicts of interest.

On a trip last week to the Nevada Gaming Control Board laboratory, in a State office building off the Las Vegas Strip, we found testing and enforcement mechanisms that go far beyond what is required for electronic voting. Among the ways gamblers are more protected than voters:

1. The State has access to all gambling software. The Gaming Control Board has copies on file of every piece of gambling device software currently being used, and an archive going back years. It is illegal for casinos to use software not on file. Electronic voting machine makers, by contrast, say their software is a trade secret, and have resisted sharing it with the states that buy their machines.
2. The software on gambling machines is constantly being spot-checked. Board inspectors show up unannounced at casinos with devices that let them compare the computer chip in a slot machine to the one on file. If there is a discrepancy, the machine is shut down, and investigated. This sort of spot-checking is not required for electronic voting. A surreptitious software change on a voting machine would be far less likely to be detected.
3. There are meticulous, constantly d standards for gambling machines. When we arrived at the Gaming Control Board lab, a man was firing a stun gun at a slot machine. The machine must work when subjected to a 20,000-volt shock, one of an array of rules intended to cover anything that can possibly go wrong. Nevada adopted new standards in May 2003, but to keep pace with fast-changing technology, it is adding new ones this month.

   Voting machine standards are out of date and inadequate. Machines are still tested with standards from 2002 that have gaping security holes. Nevertheless, election officials have rushed to spend hundreds of millions of dollars to buy them.
4. Manufacturers are intensively scrutinized before they are licensed to sell gambling software or hardware. A company that wants to make slot machines must submit to a background check of six months or more, similar to the kind done on casino operators. It must register its employees with the Gaming Control Board, which investigates their backgrounds and criminal records.

   When it comes to voting machine manufacturers, all a company needs to do to enter the field is persuade an election official to buy its equipment. There is no way for voters to know that the software on their machines was not written by programmers with fraud convictions, or close ties to political parties or candidates.
5. The lab that certifies gambling equipment has an arms-length relationship with the manufacturers it polices, and is open to inquiries from the public. The Nevada Gaming Control Board lab is a State agency, whose employees are paid by the taxpayers. The fees the lab takes in go to the State's general fund. It invites members of the public who have questions about its work to call or e-mail.

   The federal labs that certify voting equipment are profit-making companies. They are chosen and paid by voting machine companies, a glaring conflict of interest. The voters and their elected representatives have no way of knowing how the testing is done, or that the manufacturers are not applying undue pressure to have flawed equipment approved. Wyle Laboratories, one of the largest testers of voting machines, does not answer questions about its voting machine work.
6, When there is a dispute about a machine, a gambler has a right to an immediate investigation. When a gambler believes a slot machine has cheated

him, the casino is required to contact the Gaming Control Board, which has investigators on call around the clock. Investigators can open up machines to inspect their internal workings, and their records of recent gambling outcomes. If voters believe a voting machine has manipulated their votes, in most cases their only recourse is to call a board of elections number, which may well be busy, to lodge a complaint that may or may not be investigated.

Election officials say their electronic voting systems are the very best. But the truth is, gamblers are getting the best technology, and voters are being given systems that are cheap and untrustworthy by comparison. There are many questions yet to be resolved about electronic voting, but one thing is clear: a vote for president should be at least as secure as a 25-cent bet in Las Vegas.

Chairman EHLERS. Thank you, Mr. Holt. As you well know, normally Members are not questioned by their colleagues, because we have ample opportunities to discuss it with you.

I would just add one quick comment to illustrate the difficulty of what you are referring to, and that is that I have also programmed computers many times—it is even possible to program the computer to present to the voter a verifiable notification of some sort, and yet record a different result in the memory, and so that—even that verification has difficulties. So, we have a lot of problems to deal with, but thank you very much for your testimony. I appreciate—you certainly——

Mr. BOEHLERT. Mr. Chairman, is this the witness and the Chair 100 percent of the House physicists caucus?

Mr. HOLT. This you see before you the bipartisan physics caucus of the 108th Congress.

Chairman EHLERS. And as soon as we can find a phone booth for the straw court, we will have our office.

Mr. BOEHLERT. Well, thank you, Dr. Ehlers, and thank you, Dr. Holt.

Chairman EHLERS. Thank you. Thank you very much. Thank you for coming, Mr. Holt.

Mr. BAIRD. Mr. Chairman, if I may. Mr. Chairman. I would just like to express my profound respect and appreciation for the gentleman's work.

Chairman EHLERS. Yes.

Mr. BAIRD. I can tell you, I receive letters and phone calls from constituents who are profoundly concerned about this, and there are no PACs, there are no political contributions that go with is. This is a Member of the Congress fighting for a fundamental principle of one person, one vote, and that votes be fairly counted, and I have a tremendous admiration and gratitude for the gentleman, and we all owe him, as Americans, a debt of appreciation.

Mr. HOLT. Thank you. I thank Mr. Baird. And I would say, Mr. Udall said that this may seem to be a dry topic. Let me tell you that this is a topic that has excited hundreds of thousands, if not millions of Americans. Since four years ago, I think we have had an education here in the United States about voting, and it has excited many people, and I am certainly pleased to see that so many Americans believe their vote is sacred, and they are taking steps to see that their votes are protected.

Chairman EHLERS. I thank you for your comments, your testimony, and let me assure you this subcommittee shares that. That is why we wrote the legislation two years ago, and wish it had been even stronger in the final version, and fully funded. Thank you for being here.

If there is no objection, all additional opening statements submitted by the Subcommittee Members will be added to the record. Without objection, so ordered.

We will now ask the second panel to take their places at the table. At this time, I would like to introduce our second panel of witnesses. Mr. Tom Wilkey is the Chair of the National Association of State Election Directors, also known as NASED, and he is Chair of the Independent Testing Authority Committee, I believe. Ms. Carolyn Coggins is the Director of ITA Services at SysTest Labs,

an Independent Testing Authority for software, based in Boulder, Colorado. Dr. Michael Shamos is a Professor of Computer Science at Carnegie Mellon University. And a familiar face, Dr. Hratch Semerjian, is the Acting Director of the National Institute of Standards and Technology.

As our witnesses presumably have already been told, you will each have five minutes to offer your spoken testimony. If your written testimony is longer than that, we ask you to summarize it within the five minute time periods. And after you complete your five minutes, then we will each question you, and each of us will have five minutes to do so. The timer, in case you haven't been told, will display green during the first four minutes of your talk, yellow during the last minute, and red, all sorts of exciting things happen. So try to wrap up before it turns red.

At this point, we will open our first round. Mr. Wilkey, you may proceed. Would you please turn on your microphone?

Panel II

STATEMENT OF MR. THOMAS R. WILKEY, CHAIR, INDEPENDENT TESTING AUTHORITY (ITA) COMMITTEE, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS

Mr. WILKEY. Thank you, Mr. Chairman, and I am Thomas Wilkey. I am the former Executive Director of the New York State Board of Elections, having retired from that position last August. However, I continue to chair the NASED Voting Systems Board, and I am pleased to appear before you today to discuss the work that has been done by the National Association of State Election Directors, NASED, with regards to the selection of Independent Test Authorities, and its program to encourage states to adopt the federal voting system standards, and to utilize test reports which have been issued by these ITAs.

My involvement in the development of the Federal Voting System Standards began several years before NASED became an official organization. Several of my colleagues worked with me on an advisory panel in assisting the FEC in the development of the first set of voluntary standards in 1990. These standards were developed over a 5-year period, between 1985 and 1990, and the initial drafts were contracted to the late Robert Naegele of Granite Creek Technology, who had for many years worked in the area of voting system testing for the State of California.

Following the adoption of the standards in 1990, it became evidence that states were not adopting these standards. Because the Federal Government was not interested in the selection of qualified Independent Testing Authorities, the standards were destined to lie on a shelf collecting dust, and the hard work of developing them would have been in vain. At that time, NASED was formed, and at one of their earlier meetings, discussions took place to try to develop a program that would encourage member States to adopt the standards, select and qualify testing laboratories that would not only test equipment and software, but provide reports to states which needed them as a component of their own certification process.

Identifying laboratories qualified to do this testing, and by having member States participate in this program, vendors would need only go to one or two laboratories to have comprehensive testing completed, thus saving time and money by avoiding duplicate testing in each state.

Needless to say, our plans did move quickly in those early years, as it was difficult to find laboratories that were willing to do the work, given the economic realities of the times, and a somewhat less than perfect fit into their overall business plans.

At the outset, a handbook was developed by Bob Naegele, which was utilized as a checklist for prospective laboratories, outlining the necessary personnel and equipment to do the work. This handbook was revised several years ago, and a copy has been provided to the Committee.

NASED was very pleased that Wylie Laboratories in Huntsville, Alabama stepped up to the plate to become our first ITA. Their expertise in the testing of hardware and software for NASA and other U.S. government agencies is internationally recognized, and they have continued to this day to work with us toward the qualification of numerous voting systems in use throughout the country.

Over the years, Wylie has been joined by Ciber, Inc. of Huntsville, Alabama, and SysTest Laboratories of Denver, Colorado, who have been qualified as software laboratories. SysTest has recently been qualified to test hardware as well, and joins us today in our presentation to the Committee.

Over the years, while we have encouraged other laboratories to join this project, the consideration of the sheer volume of business and the negative publicity of late caused most others to decline this opportunity. We continue to encourage others to look at this program as we transition this program to the Election Assistance Commission and to NIST in the next several months.

NASED's involvement in the development of the 2002 standards was twofold. In the late 1990's, NASED requested the FEC provide funding for revisions that NASED thought were needed, based on the testing and evaluation that had been done over the past several years, and the fact that standards were now nearly 10 years old. New technology and issues not considered in the original standards needed to be addressed.

The FEC acted on our request and authorized a contract with Mantec, Incorporated, to conduct a needs assessment and evaluation to determine if the project indeed needed to be done, and if so, the scope of the work to be done.

As a result of the needs assessment, the FEC awarded a contract to AMS Consulting to draft the revised standards and prepare them for a series of public comment periods required by federal law. NASED's contribution to the project included the involvement of NASED's Voting Systems Standards Board, as members of an ad hoc advisory group.

It is important for the Committee to understand several important facts as they relate to NASED's role in the selection of ITAs.

First, there is a misconception that NASED certifies voting equipment, or voting systems. NASED's role is solely limited to review and qualify perspective ITAs, and provide for the review of reports by its technical subcommittee before they are sent to the ven-

dors, and to, ultimately, State ITAs and others designated by states to receive and review them.

NASED, through its Secretariat, who for many years, had been the Election Center, had placed on its web sites information regarding systems which had been qualified under the standards, so that States and local jurisdictions, particularly those who had no formal certification process, could know that a system had met the voluntary federal voting system requirements. This secretarial role was turned over to the Election Assistance Commission in November of 2003.

Member of NASED's Voting System Board served on a voluntary basis, receiving no salary or compensation, and in many cases, traveling at their own expense to intense sessions held on weekdays or on weekends in Huntsville, or in other areas across the country. The Election Center received no compensation whatsoever, except for reimbursement of room expenses. The sum and substance of this was that this program operated on a purely voluntary basis without any funding from the Federal Government, nor, with the exception of the travel expenses for some members, without any State or local funding.

NASED has worked closely since January of 2003 with NIST on the transition of this program to the Technical Guidelines Development Committee, under the Election Assistance Commission. Regular meetings will hopefully provide for a smooth transition and eventual reevaluation of ITAs by the EAC and NIST, and the consideration of other issues which we have dealt with as part of our program.

NASED is proud of what we have tried to accomplish. We know that there have been weaknesses in the program, but that it is finally the day to get the day to day full-time attention that is needed under the EAC and NIST.

Voting System Board members, election directors, and dedicated experts in the field of technology have given thousands of hours of their personal time and talent to this program, because they wanted to make a difference.

Together, colleagues rose to meet a tremendous challenge, with a single goal in mind, to help ensure the integrity of America's voting systems and processes. Absent these bold motives almost 15 years ago, recent scenarios would have been significantly worse.

Many people have said to me over the past several months that given the current media attention on voting systems, it would have been understandable had we thrown in the towel on this critical issue. But looking back, I can say with confidence that we can be proud of what we accomplished, as we tried to do something rather than nothing at all.

Thank you for the opportunity to testify today and for your interest in this matter.

[The prepared statement of Mr. Wilkey follows:]

PREPARED STATEMENT OF THOMAS R. WILKEY

Mr. Chairman and Members of the Committee;

I am pleased to have the opportunity to appear before you today to discuss the work that has been done by the National Association of State Election Directors (NASED) with regards to the selection of Independent Test Authorities (ITA) and

it's program to encourage states to adopt Federal Voting System Standards and utilize test reports which have been issued by these ITAs.

My involvement in the development of the Federal Voting System Standards began several years before NASED became an official organization. Several of my colleagues worked with me on an Advisory panel in assisting the FEC in the development of the first set of voluntary Standards in 1990.

These standards were developed over a five-year period (1985–1990) and the initial drafts were contracted to the late Robert Naegele of Granite Creek Technology who had for many years, worked in the area of voting system testing for the State of California.

Following the adoption of the standards in 1990, it became evident that States were not adopting the standards. Because the Federal Government was not interested in the selection of qualified Independent Testing Authorities, the standards were destined to lie on a shelf, collecting dust and the hard work of developing them would have been in vain.

At that time NASED was formed, and at one of their earlier meetings, discussions took place to try to develop a program that would encourage member States to adopt the standards, select and qualify testing laboratories that would not only test equipment and software, but provide reports to states which needed them as a component of their own certification process.

By identifying laboratories qualified to do this testing and by having member States participate in the program, vendors would only need to go to one or two laboratories to have comprehensive testing completed, thus saving time and money by avoiding duplicative testing in each state.

Needless to say our plans did not move quickly in these early years, as it was difficult to find laboratories that were willing to do the work, given the economic realities of the times, and a somewhat less then perfect fit into their overall business plans.

At the outset, a handbook was developed by Bob Naegele which was utilized as a check list for prospective laboratories, outlining the necessary personnel and equipment to do the work. The handbook was revised several years ago and a copy has been provided to the committee. Mr. Steve Freeman, who joins me on the panel today is here to briefly outline the steps taken to qualify a test laboratory as he has been involved in this task for NASED and has received training under the National Institute of Standards and Technology (NIST) to do so in future evaluations.

NASED was very pleased that Wylie Laboratories in Huntsville, Alabama stepped up to the plate to become our first ITA. Their expertise in the testing of hardware and software for NASA and other U.S. Government agencies is internationally recognized and they have continued to this day to work with us toward the qualification of numerous voting systems in use throughout the country.

Over the years, Wylie has been joined by Ciber Inc. of Huntsville, Alabama and SysTest Laboratories of Denver, CO. who have been qualified as software laboratories. SysTest has recently been qualified to test hardware as well and joins us today in our presentation to the Committee.

Over the years, while we have encouraged other laboratories to join this project, their consideration of the sheer volume of business and the negative publicity of late, caused most others to decline this opportunity. We continue to encourage others to look at this program and as we transition this program to the Election Assistance Commission and to NIST in the next several months we know that they will be reaching out to all interested parties as well.

NASED's involvement in the development of the 2002 standards was two-fold:

In the late 1990's NASED requested that the FEC provide funding for the revisions that NASED thought were needed, based on the testing and evaluation that had been done over the past several years and the fact that the standards were now nearly ten years old. New technology and issues, not considered in the original standards needed to be addressed.

The FEC acted on our request and authorized a contract with Mantec Inc. to conduct a needs assessment and evaluation to determine if the project indeed needed to be done and if so, the scope of the work to be done.

As a result of the needs assessment, the FEC awarded a contract to AMS Consulting to draft the revised standards and prepare them for a series of public comment periods required by federal law. NASED's contribution to the project included the involvement of NASED's Voting System Standards Board as members of an ad hoc advisory group to review the document and make suggestions for improvement. The 2002 Standards were released in the fall of that year.

It is important for this Committee to understand several important facts as they relate to NASED's role in the selection of ITAs, the development of standards, and our overall program.

First, there is a misconception that NASED "certifies" voting systems. NASED's role is solely to review and qualify prospective ITAs and provide for the review of reports by it's technical subcommittee, before they are sent to the vendors and ultimately to State ITAs and others designated by the states to receive and review same.

NASED, through it's secretariat, who for many years has been the Election Center, has placed on its web sites, information regarding systems which had been qualified under the standards, so that States and local jurisdictions, particularly those who had no formal certification process, can know that a system has met the voluntary federal voting system requirements. This secretariat role was turned over to the Election Assistance Commission in November 2003.

Members of NASED's voting system board served on a voluntary basis, receiving no salary or compensation and in many cases traveled at their own expense to attend sessions held on weekdays as well as weekends in Huntsville and the Election Center served as our Secretariat did so without any compensation, except for the reimbursement of meeting room expenses. The sum and substance of this was that this program operated on a purely voluntary basis without any funding from the Federal Government, nor with the exception of travel expenses for some members, without any State or local funding.

NASED has worked closely since January of 2003 with NIST on the transition of this program to the Technical Guidelines Development Committee under the Election Assistance Commission. Regular meetings will hopefully provided for a smooth transition, and the eventual re-evaluation of ITAs by the EAC and NIST, and the consideration of other issues which we have dealt with as part of our program.

NASED is proud of what we have tried to accomplish. We know there have been weaknesses in the program, but that it will finally get the day-to-day full-time attention that it needed but never realized under the voluntary nature of our program.

Voting System Board members, election directors and dedicated experts in the field of technology have given thousands of hours of their personal time and talent to this program because they wanted to make a difference. Together, colleagues rose to meet a tremendous challenge, with a single goal in mind—to help ensure the integrity of America's voting systems and processes. Absent those bold motives almost 15 years ago, recent scenarios would have been significantly worse.

Many people have said to me over the past several months, that given the current media attention on voting systems, it would have been understandable had we thrown in the towel on this critical issue. But looking back, I can say with confidence that we can be proud of what we accomplished, as we try to do something rather than nothing at all.

Thank you for the opportunity to testify today and for your interest in this important matter.

Chairman EHLERS. Thank you for your comments. Ms. Coggins.

STATEMENT OF MS. CAROLYN E. COGGINS, DIRECTOR, ITA SERVICES AT SYSTEST LABS

Ms. COGGINS. Mr. Chairman and Members of the Committee, I am Carolyn Coggins from SysTest Labs. We are the only combined hardware and software NASED Independent Test Authority. Thank you for inviting us here today to speak about qualification testing.

NASED qualification testing is, to the 2002 FEC Voting System Standards. All testing conforms to two VSS processes. This first is the physical configuration audit. It addresses the source code, software, hardware configuration, and documentation.

The functional configuration audit addresses all testing. SysTest has created a test methodology incorporating physical and functional configuration audit-specific reviews and tests. Standard templates are customized for each unique voting system, but the overall process is always the same for every voting system.

To have confidence in the voting system, one needs to have confidence in the testing. NASED qualification testing is the second level of four levels of testing identified by the Voting System Standards. The first level of testing is vendor testing. The vendor tests to the design requirements. The second level is qualification testing. The ITAs examine the vendor's testing for adequacy and completeness. We run a standard set of end-to-end functional tests customized for the specific voting system to ensure that it meets the VSS. We also test for any additional functionality that is non-VSS required.

Qualification testing means that the hardware, software, and all documentation of the voting system have been defined, reviewed, and tested for conformance with the requirements of the Voting System Standards. It means the voting system contains a method to create elections, provide a ballot, record votes, report tallies, and produce an audit trail. It means voting is secret, accurate, and reliable. It means all code used in testing has been reviewed by an ITA, and it means that the documentation required to help jurisdictions run elections is accurate and sufficient.

The qualification testing does not mean that testing has been sufficient to confirm that voting systems meet the specific laws of all states, or for that matter, any State. This responsibility falls to the third level of testing, State certification. Qualification testing also does not mean that the voting system the vendor delivers is exactly the system that was qualified or certified. This aspect falls to the fourth level of testing, local acceptance testing.

All four levels are essential to the voting process. We suggest that the 1990 Voting System Standard implementation plan be used as a baseline guide. While never fully implemented, it contains an excellent structure for issues associated with all levels of voting testing. Additionally, we recommend that the new EAC standards define specific reporting methodologies and poll worker usability, to assist the States and local jurisdiction to understand and use ITA qualification reports and voting systems themselves.

To ensure confidence in testing, you have to have confidence in the test labs. Currently, environmental testing and all functional software and hardware testing of the polling place equipment is assigned to the hardware ITA. The functional testing of ballot preparation and the central count functionality, and then the integration of end-to-end testing is assigned to the software ITA.

As technology has evolved, we feel this scope should be reexamined, because polling place software cannot be fully tested without integrating ballot preparation and counting software. Integration testing repeats much of the polling place functional testing. New voting systems today tend not to have separate applications that neatly divide these functions. Vendors must artificially divide code in order to conform to current lab assignments. Lastly, polling place issues that are found in end-to-end testing by a software ITA must go back to the hardware ITA for code review and functional testing. Then, the hardware ITA must send the code back to the software ITA to rerun their tests.

The Subcommittee has asked us to provide suggestions for future accreditation of labs. We would suggest that the accrediting of primary labs responsible for all hardware and software testing. We

would also suggest that primary labs may have qualified subcontractors to perform environmental testing, but they must demonstrate their ability to monitor all subcontractor work.

Lastly, to ensure confidence in voting systems testing and labs, one must have confidence in the standards. Criticism of the 2002 standards generally is focused on security in terms of active attack code such as backdoors. When you look at security from a broader view, the requirements of the VSS are more comprehensive. Testing for accuracy and reliability helps secure the vote. Testing the functional requirements dealing with election creation, voting, counting, and auditing helps secure the vote. Documenting the processes to ensure physical security and detect intrusion help secure the vote.

In terms of active attack code, the VSS supplies some detail, and there are some sections that provide very wide latitude to the labs. These sections give the individual labs a great deal of discretion, but it does not provide the detail consistency across all ITAs. The role of the ITA is to hold the vendor's feet to the fire, but it is not to build the fire. HAVA tasks the EAC in this to address this issue in the future.

The Subcommittee has asked us to provide suggestions for changes to improve the process before the 2006 Election. The 2002 VSS implementation plan has a process for issuing clarification bulletins. We would suggest a NASED, EAC, and NIST transition clarification bulletin addressing any significant issues.

Thank you for the opportunity to speak here, and we thank you.

[The prepared statement of Ms. Coggins follows:]

PREPARED STATEMENT OF CAROLYN E. COGGINS

SysTest Labs is pleased to provide the Environment, Technology, and Standards Subcommittee with information about ITA (Independent Testing Authority) Qualification Testing of Voting Systems for the National Association of State Election Directors (NASED) to the Federal Election Commission (FEC) Voting System Standards (VSS).

Three labs currently provide NASED Qualification Testing. All of the labs test to the VSS, but each has their own methods. Our comments here reflect the methods used by SysTest Labs.

My discussion shall identify:

- SysTest Labs' qualifications and accreditation as an ITA;
- The standards, in addition to the VSS, that govern qualification testing;
- How the Voting System Qualification Test process is defined in the VSS;
- How SysTest Labs implements the VSS Voting System Qualification Test process;
- How SysTest Labs maintains quality and manage process improvement; and
- Observations and recommendations regarding lab accreditation, the VSS and qualification testing.

Accreditation as a NASED Qualification ITA

SysTest Labs is full service laboratory specializing in all areas of software testing. Our work ranges from Independent Verification and Validation for software development efforts of State unemployment insurance systems to large and complex software laboratory testing for major telecommunication companies to web site performance testing for major retailers to software test staff augmentation. SysTest Labs has successfully completed over 500 software testing or quality assurance projects for over 250 clients worldwide. Regardless of the test effort, all aspects of our quality program, test methodology and test engineer training are guided by Institute of Electrical and Electronic Engineers (IEEE) standards and the SysTest Labs quality procedures.

In order to become a software and hardware ITA, SysTest Labs had to apply to NASED and then be audited by the NASED Technical Committee. To my knowledge, we are the only lab that has sought and been awarded both software and hardware accreditation, to become a full service ITA. We initially applied and qualified as a software ITA in 2001. We recently granted acceptance as a hardware ITA. Our hardware ITA status is provisional, i.e., our audit was successfully completed, NASED has recommended accreditation and our initial hardware qualification test effort will be monitored by a NASED auditor.

Quality Program, Test Standards and Test Methods

The NASED audit process requires that we provide documentation and demonstrate our quality program. In addition, we have had to provide documentation and demonstrate our test methodology and processes for NASED Qualification Testing of voting systems. While the requirements we test to are governed by the standards, we must define the method of testing and processes to ensure the consistency, adequacy, accuracy, and overall quality of our NASED Qualification Testing.

While the 2002 Federal Election Commission Voting System Standard is the primary standard, there are a number of other standards used in our voting system testing. The VSS itself incorporates a number of other standards, which are included in NASED Qualification Testing (see Volume 1 Applicable Documents). The primary standards we use in NASED ITA Qualification Testing are:

Federal Election Commission

- Federal Election Commission Voting System Standards, Volume I Performance Standards and Volume II Test Standards, April 2002.

National Association of State Election Directors

- NASED Accreditation of Independent Testing Authorities for Voting System Qualification Testing, NASED Program Handbook NHDBK 9201, a National Association of State Election Directors (NASED), May 1st, 1992.
- NASED Voting System Standards Board Technical Guide #1, FEC VSS Volume I, Section 2.2.7.2, Color and Contrast Adjustment
- NASED Voting System Standards Board Technical Guide #2, Clarification of Requirements and Test Criteria for Multi-language Ballot Displays and Accessibility.

Institute of Electrical and Electronics Engineers

- IEEE Standard for Software Quality Assurance Plans IEEE STD 730–1998
- IEEE Standard for Software Configuration Management Plans IEEE STD 828–1998
- IEEE Standard for Software Test Documentation IEEE STD 829–1998
- IEEE Recommended Practice for Software Requirements Specifications IEEE STD 830–1998
- IEEE Standard for Software Unit Testing IEEE STD 1008–1987
- IEEE Standard for Software Verification and Validation IEEE STD 1012–1998.

Federal Regulations

- Code of Federal Regulations, Title 20, Part 1910, Occupational Safety and Health Act
- Code of Federal Regulations, Title 36, Part 1194, Architectural and Transportation Barriers Compliance Board, Electronic and Information Technology Standards—Final Rule
- Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission
- Code of Federal Regulations, Title 47, Part 15, "Radio Frequency Devices," Subpart J, "Computing Devices," Rules and Regulations of the Federal Communications Commission.

American National Standards Institute

- ANSI C63.4 Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9Khz to 40 GHz
- ANSI C63.19 American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids.

International Electro-technical Commission.

Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques

- IEC 61000–4–2 (1995–01) Section 2 Electrostatic Discharge Immunity Test (Basic EMC publication)
- IEC 61000–4–3 (1996) Section 3 Radiated Radio-Frequency Electromagnetic Field Immunity Test
- IEC 61000–4–4 (1995–01) Section 4 Electrical Fast Transient/Burst Immunity Test
- IEC 61000–4–5 (1995–02) Section 5 Surge Immunity Test
- IEC 61000–4–6 (1996–04) Section 6 Immunity to Conducted Disturbances Induced by Radio-Frequency Fields
- IEC 61000–4–8 (1993–06) Section 8 Power-Frequency Magnetic Field Immunity Test. (Basic EMC publication)
- IEC 61000–4–11 (1994–06) Section 11. Voltage Dips, Short Interruptions and Voltage Variations Immunity Tests.

Electromagnetic compatibility (EMC) Part 5–7: Installation and mitigation guidelines

- IEC 61000–5–7 Ed. 1.0 b: 2001 Degrees of protection provided by enclosures against electromagnetic disturbances.

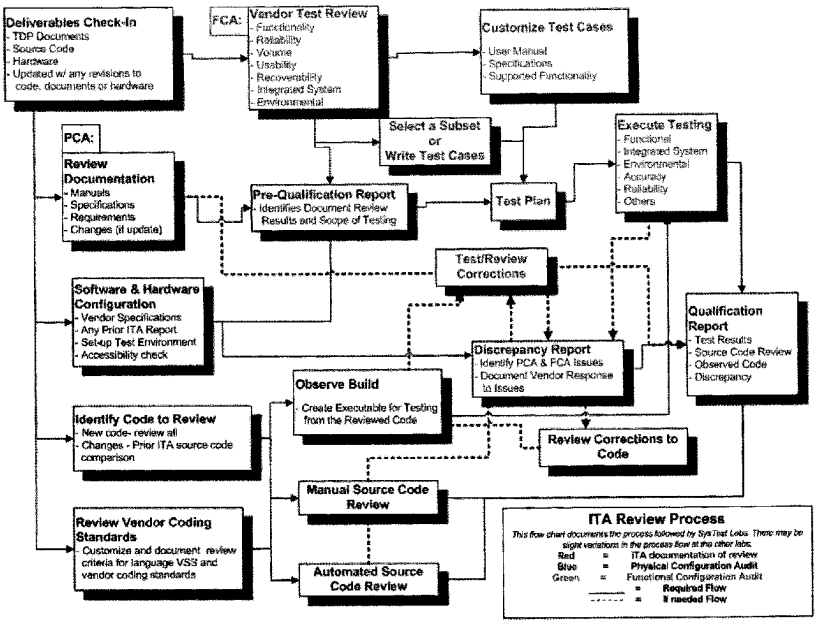
Military Standards

- MIL–STD–810D (2) Environmental Test Methods and Engineering Guidelines.

NASED Qualification Testing of Voting Systems ITA Process

SysTest Labs performs qualification testing in conformance with the two processes required in the 2002 VSS. The results from Qualification reviews and testing are documented throughout the process (ITA documentation of testing in red):

- Physical Configuration Audit (PCA in blue) addresses the physical aspects of the voting system, including:
  - Review of the Technical Data Package (TDP) documentation
  - Verification of the configuration of the hardware and software
  - Identification of the code to review
  - Source Code review
  - Observing the building of the executable from the reviewed source code.
- Functional Configuration Audit (FCA in green) addresses the functional aspects of the voting system, including:
  - Review of all testing performed by the vendor
  - Test planning
  - Test Case preparation and/or customization of Standard Test Cases
  - Test execution.



While the VSS outlines the overall PCA and FCA process, SysTest Labs has defined specific processes for each area of testing or review to ensure a consistent, repeatable test methodology. These processes include specific review and test templates that have been prepared in conformance with the VSS, IEEE standards, NASED accreditation policies and SysTest Labs quality procedures. Each voting system is unique. While qualification testing must be customized for the unique requirements of each specific voting system, the overall process is exactly the same for every voting system.

The VSS does not designate software and hardware ITA responsibilities. These responsibilities are assigned by NASED accreditation policies. The processes documented here note processes or test approaches that can be applied to either the software or hardware ITA.

- **PCA Technical Data Package (TDP) Review:** The TDP is reviewed to confirm required documentation is present, conforms in content/format and is sufficient to install, validate, operate, maintain the voting system and establish the system hardware baseline associated with the software baseline. Results of the review are provided to the vendor in a Pre-qualification Report.
- **PCA Source Code Review:** The source code is reviewed for:
  - Maintainability—including the naming, coding and comment conventions, adherence to coding standards and clear commenting.
  - Control Constructs—to determine the logic flow utilizes standard constructions of the development language, its used consistently, the logic structure isn't overly complex and there's an acceptable use of error handlers. Where possible automated tools are used.
  - Modularity—confirming each module has a testable single function, unique name, single entry/exit, contains error handling and an acceptable module size.
  - Security and Integrity of the Code—including controls to prevent deliberate or accidental attempts to replace code such as unbounded arrays or strings, including buffers to more data, pointer variables and dynamic memory allocation and management; and other security risks, such as hard coded passwords.

- **PCA Test Environment:** The Hardware and Software ITAs document the setup of the voting system configuration to assure a consistent test environment. The ITAs observe building of the executable from reviewed source code. The Hardware and Software ITAs work together to confirm that all testing is performed only on ITA reviewed code built under ITA observation.
- **FCA Test Documentation Review:** The ITA reviews and assesses prior testing performed by the vendor. Based upon the assessment of vendor testing the ITA identifies scope; designs testing; and creates the Qualification Test Plan.
- **FCA Testing:** Each ITA tests to their identified scope, using their own internal processes.
    - **Polling Place System Testing:** The Hardware ITA initiates environmental operating and non-operating tests; functional testing of polling place hardware/software, and user manuals for all VSS-required and optional vendor supported functionality; testing the capability of the voting system to assist voters with disabilities or language; and accuracy and reliability testing.
    - **Election Management System Testing:** The Software ITA initiates functional testing of the Ballot Preparation and Central Count hardware/software, and user manuals for all VSS-required and optional vendor supported functionality.
    - **System Level Testing:** The Software ITA initiates end-to-end testing of the integrated EMS and Polling Place System, including testing of the system capabilities and safeguards, claimed by the vendor in its TDP.

Creating the Test Methodology and Maintaining Quality

In structuring our review and test methodology we are guided by a continual quest to improve the process and quality. From the foundation of our first ITA project we have continually examined our methods. Through ten completed or active projects we have honed and revised our processes. Some changes have been based upon internal 'lessons learned' and others have come from the external changes in the ITA process, such as the update to the 2002 VSS.

The process we followed in creating and maintaining the NASED Qualification Testing was to define and document a review and test process for both management and test activities. This process needed to be standardized, repeatable and integrated into the overall structure for all SysTest Labs testing projects. Within this standard structure we tailored the individual methods to the unique requirements of software ITA qualification testing based upon the 1990 VSS. Processes addressed in this phase included VSS requirements management, test elements (plans, test cases, reviews and reports), test management, defect tracking, basic training, quality assurance, configuration management (vendor materials and our testing) and project management.

Our next step was to work with and observe and improve the process through successive test efforts. In this phase we broadened our view to training needs, organizational coordination of the individual test tasks and peer reviews. With each effort we reworked some processes and identified other areas for potential process improvement.

At the point the 2002 VSS was implemented, we had a solid structure and the perfect opportunity to implement several identified process improvements, in conjunction with a conversion to the new standards.

While we continue to observe our processes, we are also moving into an optimization phase. In our expanded role as a hardware ITA we will be initiating some new processes that will follow our historic model, but will also look at some of our old processes and optimize them for an increased workload.

Observations and Recommendations for Lab Accreditation

The majority of VSS requirements for qualification testing involve software. There are unique environmental tests that address hardware specifically, but the VSS requires that a portion of software testing for accuracy and reliability be performed in environmental chambers. In doing so there is an overlap. The most effective way to handle this overlap is to create a structure that permits joint testing of the hardware and software. NASED structured the scope of testing so that the hardware ITA was responsible for functional software and hardware testing on the polling place equipment and environmental testing of the hardware. The software ITA has been responsible for the ballot preparation and central count functionality along

with integration testing of the entire system (end-to-end elections processes). While the software ITA does not review all the code, they must receive all of the code in order to perform end-to-end testing on the integrated system.

We feel this scope should be changed due to the following issues:

- Polling place software cannot be fully tested without integrating the entire voting system. Today's new voting system vendors do not develop separate applications. In the majority of systems we see, a vendor is forced to artificially divide their code in order to give the polling place software to the hardware ITA and the balance to the software ITA.
- The ITA labs try to keep duplication of effort down to a minimum, however integration testing must repeat much of the polling place functional testing.
- Vendors are required to return to the hardware ITA for regression testing if issues are uncovered during integration testing. If the software ITA uncovers an issue in the polling place during integration testing, they must notify the hardware ITA. While the software ITA must rerun their tests with the new version of the code, the hardware ITA is responsible for reviewing the code changes to fix the issue and functionally testing to confirm the fix. In addition, there have been times when ITA labs have an inconsistent interpretation of the standards and a vendor's solution will overlap between the hardware and software ITA.
- While environmental hardware testing requires specialized equipment and testing, the environmental test methodology is not unique to voting systems and generally does not require specialized knowledge of voting. Furthermore, effective software testing does require specialized knowledge of voting practices.

We recommend that accreditation of labs include the following:

- Primary labs that bear responsibility for all testing, review and reporting. Primary labs may have qualified subcontractors to perform specialized testing, e.g., hardware environmental testing. The primary lab must demonstrate their ability to monitor the work of the subcontractors and verify that all subcontractor work reflects quality processes equal to or greater than those of the primary lab;
- Validation of an understanding of the unique functional requirements of voting systems and voting system standards;
- Validation of manual and automated software testing experience, methodology and software quality engineering practices meet a minimum of CMMI Level 3; and
- Validation of test equipment and chambers sufficient to perform all VSS defined environmental testing, as well as environmental testing experience, methodology and quality engineering practices.

Observations and Recommendations for Voting System Standards

One hears much discussion on the adequacy of the 2002 FEC Voting System Standards with extensive criticism against the adequacy of security standards, but perhaps these critics are not taking a broad view of how the VSS addresses security. Basic functionality requirements, such as printing the name of an election and date on all reports, are an aspect of security. Voting system, accuracy and reliability are aspects of securing the vote. Any functional requirement of the VSS that deals with election creation, voting, counting or auditing is an aspect of securing the vote. The VSS requirement for a vendor to identify the weight of paper deals with the security of the vote. Additionally, the VSS requirements call for documentation of the process to ensure physical security of a voting system and the ability to detect intrusion. When looked at from this broad view, the requirements of the VSS are quite comprehensive.

Criticism is generally is focused on the narrower view of security in terms of active attack code such as viruses, worms, Trojan horses, logic bombs, backdoors, exploitable vulnerabilities, and programming flaws. The VSS provides some detail here. There are also sections in the VSS that provide the labs with some wider latitude. In Volume 2 Section 1.5 the VSS states *"Additionally, new threats may be identified that are not directly addressed by the Standards or the system. As new threats to a voting system are discovered, either during the system's operation or during the operation of other computer-based systems that use technologies comparable to those of another voting system, ITAs shall expand the tests used for system security to address the threats that are applicable to a particular design of voting system."*

A statement like this allows the individual lab a great deal of discretion in testing. What it does not do is provide the detail for consistency across all ITA testing.

Is providing more detail being addressed? HAVA specifically identifies a review of the security and accessibility requirements of the VSS and creation of new voting standards by the EAC, with the support of NIST.

Is there anything that can be done to enhance the VSS without waiting for the writing of new standards? Yes. The 2002 FEC Voting System Standards Implementation Plan identified a process for issuing clarification bulletins. This year NASED Voting System Standards Board Technical Guides 1 and 2 were issued with clarifications of two VSS requirements dealing with accessibility. Although NASED has a mechanism to issue clarifications, we are not aware if they have the physical or financial resources to meet this responsibility.

In terms of the HAVA mandated review of the VSS to be performed by the EAC and NIST, we offer the following suggestions for greater guidance in the standards:

- Coding flaws—These may have security implications, such as vulnerable constructs. Some languages and their supporting libraries provide security vulnerabilities within their functions. This can allow for a buffer overflow (which is addressed in the VSS Volume 2 Section 5.4.2.d, *"For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries"*) or a stack overflow attack. Additional, and potentially more harmful, is the vulnerability to access the wrong program or data file. This makes the program susceptible to the introduction of external malicious code. We suggest providing language specific prohibitions of vulnerable constructs. Currently these vulnerable constructs can be used in programs without malicious intent but it is difficult in a static review to detect the security implication with their use.
- Race conditions—Synchronization issues, such as race conditions, present security vulnerabilities. Automated code checking tools can detect the potential for this situation but typically detect a number of "false positives." We suggest guidance on the acceptability of race conditions within the code.
- Global Variables—These variables are recognized throughout the program and in some cases are used to store critical status information that a number of programs need and therefore provide a valuable service; however, their potential for error and abuse should discourage their use. We suggest guidance on when they can and cannot be used.

We would also suggest that the standards include the following:

- Code Review Requirements for the vendors to provide documentation identifying the known security weaknesses of the programming language(s) they used, and their process for mitigating those weaknesses.
- Requirements for the vendors to provide documentation of their security practices. The standards need to also provide the ITAs with guidance for the review of this documentation to assure that security is incorporated into the vendor's development process.

Observations and Recommendations for NASED ITA Qualification Testing

The greatest challenge for NASED ITA Qualification Testing is the lack of understanding of what it is, what it is supposed to do, what it does not do and the role it should play in the entire election process.

What is NASED ITA Qualification Testing? It is the second of four levels of testing identified in the VSS.

- **Level 1 Vendor Testing:** The vendor tests to ensure that their system meets their design specifications, the requirements of the VSS, and any specifically supported State requirements.
- **Level 2 NASED ITA Qualification Testing:** The vendor's testing is reviewed for adequacy and additional testing is performed by software and hardware ITAs to ensure that the voting system meets the requirements of the VSS, and any additional functionality supported by the voting system as defined in the vendor's design specifications performs as specified.
- **Level 3 State Certification Testing:** State personnel or contractors perform testing under the direction of the State to ensure that the voting system meets *all* of the State's requirements.
- **Level 4 Acceptance Testing:** Individual jurisdictions perform testing prior to each primary or general election to ensure that the voting system operates as required.

What is the objective of NASED ITA Qualification Testing? The intent of qualification testing is to ensure that only voting systems that pass independent testing to the minimum requirements of the 2002 FEC Voting System Standards are issued a NASED Qualification Numbers. This means:

- The elements of the voting system (hardware, software, any required materials, and all documentation) have been defined, reviewed and tested for conformance with the requirements of the VSS;
- The voting system contains a method to successfully create elections, provide a ballot, record votes, provide report tallies, and produce an audit trail;
- Using the vendor's documented procedures and mandatory security processes, ensuring that voting is performed in a secret, accurate, reliable and secure manner;
- The source code has been reviewed and meets the requirements for modularity, maintainability, consistency, security, integrity, and the use of error handling;
- The code is sufficiently well commented so if the vendor cease to support the code it can be reasonably maintained by another entity;
- The code installed on the voting system for testing was built from the source code reviewed by an ITA and witnessed by an ITA;
- The Vendor's documents required by the VSS the requirements for content and format;
- The Vendor documentation required to assist the states and jurisdiction to configure, use and maintain the voting system (hardware, software, other required materials and documents) is accurate and sufficient to perform all supported functions;
- Security has been achieved through the demonstration of technical capabilities in conjunction with the documented mandatory administrative procedures for effective system security;
- Vendors have an established set of quality procedures and have supplied evidence of their implementation through development, internal testing, and ITA testing;
- The elements of the voting system configuration have been identified, tested and tracked by the ITA;
- Upon completion of testing a report has been issued to the NASED Technical Committee for peer review;
- The report has been accepted and retained by the NASED Technical Committee/EAC, the vendor and the ITA.
- NASED issued a qualification number.

What NASED ITA Qualification Testing does not mean:

- It does not mean that testing has been sufficient to confirm a voting system meets the specific laws of all the states or for that matter any state. There is much election functionality in the VSS that is optional. The VSS only requires that this work in terms of the vendor's own requirements for a function. Taking an example to the extreme, the VSS does not require a vendor to support primary or general elections; these are both optional functions. A vendor must support some sort of election, but the VSS allows the vendor to specify exactly what they choose to support.
- It does not mean that the code the vendor delivers installed on the voting system is exactly the code that was qualified. It does not mean that the hardware that was delivered by the vendor matches the qualified hardware specification. While a version number may be the same, without a verification methodology at the State and local level, it is possible for unqualified versions to be used in an election.
- While security risks are significantly reduced, it does not mean that the voting system does not require an external audit process by the local jurisdiction for detection and prevention of irregularities. The same stringent audit processes jurisdictions apply should include the voting system.

What role should NASED ITA Qualification Testing play in the election process? If one goes back to the implementation program for the 1990 Voting System Standards, one will see the direction that was originally intended. Qualification testing was just the first step. Additional phases were planned for State certification and local acceptance testing. There was a structure outlined for the accreditation

of labs by NVLAP/NIST. The FEC was supposed to be a clearinghouse to make the reports available to State and local officials. Additionally, the States and local jurisdictions were encouraged to report their certification and acceptance testing to the clearinghouse. Escrow agents were envisioned to hold qualified versions of the code and assist the States and local jurisdictions in validation of qualified versions of code.

For unknown reasons, the later phases were not implemented. NASED assumed the role for accreditation. No official clearinghouse or escrow was established. States and local jurisdictions moved forward independently. NASED informally provided a meeting place to exchange information. The job of holding the report and source code fell to the NASED ITAs. As the vendors and the ITAs had non-disclosure agreements, delivery of the report beyond the NASED Technical Committee was at the request of the vendor.

While the vendor controls delivery of the report, it does not mean State and local officials do not have the right to see the report. The report is only confidential if the State certification or a local purchaser allows it to be a confidential. We receive instructions from the vendors to send their reports to State agencies.

We would suggest that in going forward:

- The 1990 Implementation Plan shall be used as guidance in completing the future structure of the qualification, certification and acceptance testing of voting systems. Whatever structure is implemented, it must minimally address the functions outlined in this baseline plan;
- A risk and needs assessment be performed against the roles outlined in the 1990 Implementation Plan to identify the capabilities of the players to understand and perform their roles;
- The needs of the State certification and local jurisdictions for using, understanding and interpreting the qualification report should be incorporated into the new standards from the EAC. The standards should define any specific reporting methodology to assist the States and local jurisdiction in understanding the reports;
- An annually updated, centralized database of all State specific voting requirements shall be made available to the ITAs, vendors, and election officials.

BIOGRAPHY FOR CAROLYN E. COGGINS

Director of ITA Voting Services and Senior Project Manager

Carolyn Coggins has a BA in Economics from University of California, Berkeley. She heads up all voting projects at SysTest Labs and has signature authority for Independent Test Authority (ITA) Voting System recommendations to NASED (National Association of State Election Directors) for voting system approval. She serves as a ex-officio member of the NASED Technical Committee. In this capacity she provides technical assistance for NASED to the Election Assistance Commission (EAC), State election officials, and voting system vendors. Carolyn is the Chair of the Technical Data Package Special Task Group of the IEEE Project 1583 Voting Equipment Standards.

On the voting system test efforts, her responsibilities include development and maintenance of the quality processes that defines all policies, procedures and templates required to perform ITA certification testing for voting systems, ITA certification test planning development, execution, and reporting, management of ITA testing resources, and interfacing with other ITA. She communicates and enforces the policies and procedures of SysTest Labs and NASED including Test Engineering best practices for the testing of voting systems. She oversees ITA daily testing and approves the reports generated in ITA test projects. Recently she managed the efforts associated with the expansion of SysTest Labs NASED accreditation to Full ITA status including both hardware and software. In addition, Carolyn had led several highly complex testing projects for telecommunications efforts, e-commerce efforts, large migration and conversion projects. She has been with SysTest Labs since 1998.

June 21, 2004

Honorable Vernon J. Ehlers
Chairman
Subcommittee on Environment, Technology, and Standards
of the U.S. House of Representative's Committee on Science for the 108th Congress

Dear Chairman Ehlers:

This letter of financial disclosure is presented in accordance with the "Rules Governing Testimony" for witnesses appearing before the U.S. House of Representative's Committee on Science for the 108th Congress.

Since its formation on May 28, 1996, Sys.Test Labs, L.L.C. has not received any federal funding that directly supports the subject matter on which Ms. Gail Audette and Ms. Carolyn Coggins, as employees of Sys.Test Labs, L.L.C., will be testifying – namely, "Testing and Certification for Voting Equipment: How Can the Process be Improved?"

Sincerely yours

Christopher S. Hardesty
Chief Financial Officer

Chairman EHLERS. Thank you. Dr. Shamos.

STATEMENT OF DR. MICHAEL I. SHAMOS, PROFESSOR OF COMPUTER SCIENCE, CARNEGIE MELLON UNIVERSITY

Dr. SHAMOS. Mr. Chairman and Members of the Subcommittee, my undergraduate degree is in physics, and my first graduate degree is in physics, so whatever claim to omniscience that may entitle me to in this room, I gladly accept.

I have been a faculty member in the School of Computer Science at Carnegie Mellon University since 1975. I am also an attorney admitted to practice in Pennsylvania and before the U.S. Patent and Trademark Office. From 1980 until 2000, I was statutory examiner of electronic voting systems for the Commonwealth of Pennsylvania. During those 20 years, I participated in every voting system examination conducted in that state. From 1987 until 2000, I was statutory examiner of computerized voting systems for the State of Texas, and during those 13 years, I participated in every voting system examination conducted in that state. All in all, I have personally examined over 100 different electronic voting systems.

In my opinion, the system that we now have for testifying and certifying voting equipment in this country is not only broken, but is virtually nonexistent and must be recreated from scratch, or we are never going to restore public confidence in elections. The process of designing, implementing, manufacturing, certifying, selling, acquiring, storing, using, testing, and even discarding voting machines must be transparent from cradle to grave, and must adhere to strict performance and security guidelines that should be uniform for federal elections throughout the United States.

The step of qualification is testing to determine whether a particular model of voting system meets appropriate national standards. Unfortunately, no adequate standards currently exist. The Federal Voting System Standards, FVSS, formerly known as the FEC standards, are not only incomplete and out of date, but there exists no effective procedure for even repairing them.

Even if suitable standards existed, the current process of qualification testing by Independent Testing Authorities certified by NASED is not effective. As proof, I need only cite the fact that the voting systems about which security concerns have recently been raised in the popular press, such as Diebold Accuvote, were all ITA-qualified. Some of these systems contained security holes so glaring that one wonders what the ITA was doing when they were doing the testing.

Well, one may wonder, but one cannot find out. The reason for that is that the ITA procedures are entirely opaque to the public. The NASED web site contains the following peremptory statement: "The ITAs do not and will not respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system. They have neither the staff nor the time to explain the process to the public, the news media, or jurisdictions." By the way, the emphasis in that quotation was theirs, not mine. I emphasize the capitalized words from the NASED web site.

The next step, after qualification, which is certification, the process that I participated in, certification to individual State requirements, is also flawed. Many states that formerly had statutory certification procedures have abdicated them in favor of requiring no more from a vendor than an ITA qualification letter, in some cases, even less. Alabama, for example, requires no certification at all, but relies on a written guarantee by the vendor that its system satisfies that State's statutory requirements. Mind you, these are requirements over which experts may differ as to their meaning. My own State, Pennsylvania, I am embarrassed to say, abandoned certification in the year 2002, because it believed the ITA process was sufficient. We are, therefore, less safe in 2004 than we were 20 years ago, and possibly less safe than we even were in the year 2000.

Even certified machines may not operate properly when delivered to a jurisdiction, and must undergo acceptance testing, but I am not aware of any State that makes such testing a statutory requirement. It may be recommended in the standards, and the ITAs may recommend it, but there is no body that actually forces the states to go through acceptance testing.

So far, we have ignored the matter of where the software used in the machine actually comes from. It may have worked when delivered by the vendor, but may have been modified or substituted, either deliberately or innocently, by persons known or unknown. We need a central repository for election software, to which candidates and the public has continuing access, so that it may be known and verified exactly what software was used to present the ballot to the voter, and to tabulate a specific election.

I was provided in advance with three questions to which I understand the Subcommittee desires answers. One related to the accreditation of testing laboratories, and whether that should be changed to ensure greater public confidence. I believe that there certainly is room for testing laboratories. I am not against the ITA process. I just think it needs to be revamped.

Testing laboratories should be certified and rigorously monitored by the EAC, or such other national body as Congress may create. The cost of testing should be shouldered by the states on a pro rata basis, possibly out of HAVA funds. I don't believe that the laboratories should be paid by the vendors, which is the current method.

In testing laboratories, we have faced the following paradoxical situation. It is bad to have just one, because there is no competition, but it is also bad to have more than one, and the reason that is bad is that if there are multiple laboratories, undoubtedly one of them will have the reputation of being the most lax, and that is the one that every vendor would like to have examining its equipment. So, I can't decide whether there ought to be one laboratory or multiple laboratories, except that if there are multiple laboratories, and the vendor has no participation in the decision as to which laboratory will be used to test his equipment, then we would have no conflict of interest.

What can be done to improve these processes before the 2004 election, and what needs to be done by 2006? Well, the answer to the first question is simple. I don't think there's anything one can meaningfully do in the next 130 days that remain before the 2004

election. Even if it were possible to enact legislation, the states would be powerless to comply in so short a time. The saving grace, though, is that the mere presence of security vulnerabilities in voting systems does not mean that actual security intrusions will occur. We have had a successful record of using DRE machines in the United States since the late '70's. We have had a nearly perfect record of using them in Pennsylvania since 1984. There has never been a single verified incident of actual manipulation of DRE voting results in this country. We may thank our lucky stars for that. It may be happenstance that that occurred, but nonetheless, there has been a tremendous hullabaloo raised over incidents that have never actually occurred.

And how important is NIST's role in improving the way voting equipment is tested? I believe that NIST has an important role, but we are not just talking about simple electrical or mechanical specifications for equipment. We are talking about standards from beginning to end of the entire voting process, from where the machines come from, how they are deployed, how people are trained to use them, et cetera. And so I think NIST is part of the process, but the EAC, which has great election expertise, needs to be the primary force behind such processes.

Thank you very much.

[The prepared statement of Dr. Shamos follows:]

PREPARED STATEMENT OF MICHAEL I. SHAMOS

Mr. Chairman: My name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. From 1980–2000 I was statutory examiner of electronic voting systems for the Secretary of the Commonwealth and participated in every electronic voting system examination held in Pennsylvania during those 20 years. From 1987–2000 I was statutory examiner of electronic voting systems for the Attorney General of Texas and participated in every electronic voting system examination held in Texas during those 13 years. In all, I have personally examined over 100 different electronic voting systems. The systems for which I have participated in certification were used to count more than 11 percent of the popular vote in the United States in the year 2000.

I have not received any federal funding for my voting work.

I am here today to offer my opinion that the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent. It must be re-created from scratch or we will never restore public confidence in elections. I believe that the process of designing, implementing, manufacturing, certifying, selling, acquiring, storing, using, testing and even discarding voting machines must be transparent from cradle to grave, and must adhere to strict performance and security guidelines that should be uniform for federal elections throughout the United States.

There are a number of steps in the process of approving and using voting systems that must be distinguished. The process of "qualification" is testing to determine whether a particular model of voting system meets appropriate national standards. Unfortunately, no such standards currently even exist. The Federal Voting System Standards (FVSS), formerly known as the FEC Standards, are incomplete and out of date.

For example, one of the principal election security worries is the possibility of a computer virus infecting a voting system. Yet the FVSS place virus responsibility on the voting system vendor and do not provide for any testing by the Independent Testing Authority (ITA). Furthermore, the standards do not even require that a voting system contain any virus detection or virus removal software at all: "Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that

such protection is maintained in a current status." It is hardly reassuring to have the fox guarantee the safety of the chickens.

Even if there were suitable standards, it is a significant question how to assure the public that a particular machine meets them. The current process of qualification testing by Independent Testing Authorities certified by the National Association of State Election Directors (NASED) is dysfunctional. As proof I need only cite the fact that the voting systems about which security concerns have recently been raised, such as Diebold Accuvote, were all ITA-qualified. Some of these systems contain security holes so severe that one wonders what the ITA was looking for during its testing.

One may wonder, but one cannot find out. The ITA procedures are entirely opaque. The NASED web site contains this peremptory statement: "The ITAs DO NOT and WILL NOT respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system. They have neither the staff nor the time to explain the process to the public, the news media or jurisdictions." I don't believe that either Congress of the public should allow ITAs to behave this way. Did I say "ITAs"? Allow me to correct that. For hardware testing, there is only a single NASED-certified ITA: Wyle laboratories of Huntsville, Alabama. I find it grotesque that an organization charged with such a heavy responsibility feels no obligation to explain to anyone what it is doing.

It should be understood that qualification to standards addresses only one part of the problem. A qualified machine may not meet State statutory requirements even if it functions perfectly. A further examination, called certification, is needed to learn whether the machine can actually be used in a given state. Even a certified machine may fail to function when purchased unless it is tested thoroughly on delivery, a form of evaluation known as acceptance testing. I am not aware of any state that makes such testing a statutory requirement.

Assuming that the machines operate properly when delivered, there is no assurance that they will be stored, maintained, transported or set up properly so they work on Election Day. While many states provide for pre-election testing of machines, in the event of a large-scale failure they can find themselves without enough working machines to conduct an election.

The machines may work according to specification but if they have not been loaded with the appropriate set of ballot styles to be used in a polling place they will be completely ineffective. The process of verifying ballot styles is left to representatives of the political parties, who may have little interest in the correctness of nonpartisan races and issues.

In this whole discussion we have ignored the matter of where the software used in the machine comes from. It may have worked when delivered by the vendor but may have been modified or substituted, either deliberately or innocently, by persons known or unknown. We need a central repository for election software to which candidates and the public has continuous access, so it may be known and verified exactly what software was used to present the ballot and tabulate the results.

I was provided in advance with three question to which I understand the Subcommittee desires answers.

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?

Testing laboratories should be certified and rigorously monitored by the EAC, or such other national body as Congress may create. The cost of testing should be shouldered by the states on a pro-rata basis, possibly out of HAVA funds. The laboratories should certainly not be paid by the vendors, which is the current method.

In testing laboratories we face the paradoxical situation that it is bad to have just one, but it is also bad to have more than one. A single laboratory has scant incentive to do a good job, but every incentive to please its customers, namely the vendors. If there are multiple laboratories, however, then some will acquire the reputation of being more lax than others, and the vendors will seek to have their system tested by the most "friendly" laboratory. This problem can be alleviated by monitoring the performance of the laboratories and according the vendors no role in their selection.

The existence of federal standards and ITAs has actually had a counterproductive effect. Many states that formerly had statutory certification procedures have abdicated them in favor of requiring no more from a vendor than an ITA qualification letter, and in some cases even less. Alabama, for example, requires no certification at all but relies on a written guarantee by the vendor that its system satisfies the State's requirements. My own State, Pennsylvania, abandoned certification in 2002

because it believed the ITA process was sufficient. We are less safe in 2004 than we were 20 years ago.

2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?

I do not believe that Congress can act meaningfully in the 130 days that remain before the 2004 election. Even if it could, the states would be powerless to comply in so short a time. A saving race is that the mere presence of security vulnerabilities does not mean that tampering will or is likely to occur. We have been holding successful DRE elections in the U.S. for over 20 years. The problem this year is that many states, wishing to avoid the negative experience of Florida in 2000, have rushed to acquire new voting systems with which they are unfamiliar. This will undoubtedly lead to machine failures long lines, and dissatisfaction at the polls in November. It is not likely to lead to security intrusions. I should mention that since DREs were introduced in the late 1970s, there has not been a single verified incident of tampering with votes in such a system. There have been numerous allegations, all of which vanish into thin air when investigated. The most important factor right now in running a satisfactory election is training of the people who must operate the voting machines.

For 2006 there are many actions that can be taken:

- The process of conducting elections in the U.S. is highly fragmented. Election administration is left up to 3170 individual counties, except in a few states, such as Georgia, which have statewide voting systems. This means that there is a huge variance in elections budgets and level of expertise across the country. The states should be encouraged through the mechanism of HAVA to adopt systems and procedures that are as uniform as possible within each state. The more different voting systems a State operate, the more difficult it becomes to keep track of the software and firmware that is used to run them.
- No jurisdiction should be forced to deploy a new voting mechanism before it is ready. The availability of large amounts of HAVA funding has not been helpful in this regard. The rush to rid the Nation of punched-card systems, while generally laudable, has propelled counties having no experience with DRE elections into errors whose consequences will take years to overcome. A partial solution is gradual deployment and transition to the newer systems rather than overnight replacement.
- The need for voter and poll worker training cannot be over-emphasized. The best and most secure voting machine will not function properly if poll workers do not know how to operate it and voters don't know how to use it.
- A comprehensive regime of qualification, certification, acceptance and operational testing is needed.
- We need a coherent, up-to-date, rolling set of voting system standards combined with a transparent, easily-understood process for testing to them that is viewable by the public. We don't have that or anything resembling that right now, and the proposal I have heard are not calculated to install them.
- The means by which voting machines are modified, updated and provided with ballot styles and software should be tightly controlled, with meaningful criminal penalties for violations. Right now, a vendor who distributes uncertified software risks little more than adverse newspaper coverage.

3. How important is NIST's role in improving the way voting equipment is tested? What activities should States be undertaking to ensure voting equipment works properly?

I believe that NIST has an useful role to play in developing standards for voting system qualification, but it should not be a dominant one.

NIST claims to have expertise in the voting process, and cites the fact that it has produced two published reports on the subject. The first of these, which appeared in 1975, was a ringing endorsement of punched-card voting, now recognized to be the worst method of voting ever devised by man. The second report, 13 years later, corrected that error. Both, however, were written by a single individual who is not longer with NIST. The NIST voting web site, vote.nist.gov, contains a table of 16 "cyber security guidelines" that NIST asserts are responsive to the risks of e-voting. These guidelines occupy more than 2000 printed pages, yet the word "voting" appears nowhere within them.

While it is true that stringent voting machines standards are required, the task of developing them should not be assigned to NIST merely because the word "Stand-

ards" is part of its name. For voting standards are unlike any other in that they must be capable of being understood and accepted by the entire public. An airline passenger may place his trust in the pilot to verify that the plane both are about to fly in has been properly maintained. The hospital patient relies on the doctor for assurance that equipment in the operating room will not kill him. The voter has no one to turn to if her vote is not counted and therefore must develop a personal opinion whether the system is to be trusted. Suspicion about the manner of making and testing voting machines harms everyone. Arcane technical standards make the problem worse.

Having a successful, error-free and tamper-free election is not simply a matter of using a voting machine that obeys certain published criteria. Everything about the process, including the input of ballot styles, handling of vote retention devices, testing and subsequent audit must follow controlled protocols. If voting were done in a laboratory, it could be instrumented and observed carefully by engineers following precise procedures. However, voting is conducted using over one million volunteer poll workers, many of whom are senior citizens with scant computer experience. In fact, almost 1.5 percent of the U.S. voting population consists of poll workers themselves. The reality that elections are not run by engineers is an important consideration in the development and implementation of standards.

In short, expertise in the process of voting and the human factors and fears that attend that process have not historically been within NIST's expertise. I do not doubt that NIST could acquire the necessary experience given sufficient time, money and mandate. But the Nation does not have that kind of time. A repeat of the Florida 2000 experience will have a paralytic effect on U.S. elections.

Instead, I propose that standards for the process of voting be developed on a completely open and public participatory basis to be supervised by the EAC, with input from NIST in the areas of its demonstrated expertise, such as cryptography and computer access control. Members of the public should be free to contribute ideas and criticism at any time and be assured that the standards body will evaluate and respond to them. When a problem arises that appears to require attention, the standards should be upgraded at the earliest opportunity consistent with sound practice. If this means that voting machines in the field need to be modified or retested, so be it. But the glacial pace of prior development of voting standards is no longer acceptable to the public.

I may have painted a depressing picture of the state of voting assurance in the United States. That was my intention. However, I have a number of suggestions by which the process can be made to satisfy most of my concerns. In addition to the proposals presented above, I add the following:

1. There are too many organizations that appear to have authoritative roles in the voting process, including the FEC, NASED, the Election Center, NIST and the EAC. Most assert that compliance with their recommendations is voluntary, and legally it may be. But election officials abhor a vacuum, and the mere existence of published standards, good or bad, is enough to cause states to adopt them. A coherent scheme needs to be devised, at least one that will assure that voting machines work and are secure. I do not propose to sacrifice State sovereignty over voting methods and procedures so long as they are safe.
2. There is a Constitutional reluctance in the United States to having the Federal Government control elections, even those over which it may have authority to do so. I have long believed that states must be left to determine the form of voting. However, there is no contradiction in requiring that they obey minimum standards necessary to ensure that all citizens have their votes counted and moreover are confident that their votes have been counted.
3. The reality is that states cannot assume the expense of conducting multiple elections on the same day using different equipment and procedures, so if standards are mandated for elections involving federal offices they will almost certainly be used for all elections.
4. The current pall that has been cast over computerized voting in the U.S. can only be lifted through greater public involvement in the entire process.

I thank you for the opportunity to present testimony here today.

BIOGRAPHY FOR MICHAEL I. SHAMOS

Michael I. Shamos is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University, where he serves as Co-Director of the Insti-

tute for eCommerce, teaching courses in eCommerce technology, electronic payment systems and eCommerce law and regulation.

Dr. Shamos holds seven university degrees in such fields as physics, computer science, technology of management and law. He has been associated with Carnegie Mellon since 1975.

From 1980–2000 he was statutory examiner of computerized voting systems for the Secretary of the Commonwealth of Pennsylvania. From 1987–2000 he was the Designee of the Attorney General of Texas for electronic voting certification. During that time he participated in every electronic voting examination conducted in those two states, involving over 100 different voting systems accounting for more than 11 percent of the popular vote of the United States in the 2000 election.

Dr. Shamos has been an expert witness in two recent lawsuits involving electronic voting: *Wexler v. Lepore* in Florida and *Benavidez v. Shelley* in California. He was the author in 1993 of "Electronic Voting—Evaluating the Threat" and in 2004 of "Paper v. Electronic Voting Records—An Assessment," both of which were presented at the ACM Conference on Computers, Freedom & Privacy.

Dr. Shamos has been an intellectual property attorney since 1981 and has been an expert witness in Internet cases involving the Motion Picture Association of America and the Digital Millennium Copyright Act. He is Editor-in-Chief of the *Journal of Privacy Technology,* an all-digital publication of the Center for Privacy Technology at Carnegie Mellon.

Further information is available at http://euro.ecom.cmu.edu/shamos.html.

Chairman EHLERS. Thank you very much, and Dr. Semerjian.

STATEMENT OF DR. HRATCH G. SEMERJIAN, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Dr. SEMERJIAN. Thank you, Mr. Chairman, and Members of the Committee. Thank you for the opportunity to testify today on NIST responsibilities under the Help America Vote Act, specifically on testing and certification of voting equipment.

Clearly, major changes are taking place in the way we conduct elections. We are running into more and more optical scanners or touch screen systems, and as a result of these changes, Congress enacted the Help America Vote Act, commonly known as HAVA, and mandated specific roles for NIST.

Many of the issues we are examining today are directly related to standards and guidelines. Congress understood the importance of standards in voting technologies, and specifically gave the Director of NIST the responsibility of chairing the Technical Guidelines Development Committee, otherwise known, TGDC, a Committee reporting to the Election Assistance Commission under HAVA. The TGDC is charged with making recommendations to the Election Assistance Commission with regard to voluntary standards and guidelines for election-related technologies that have an impact on many of the issues we are discussing.

While we have considerable experience in standards development, NIST understands that as a non-regulatory agency, our role is limited, and we need to understand the needs of the community. To this end, NIST staff have started to meet with members of the election community. Also, at the request of Congress and the National Association of State Election Directors, NIST organized and hosted a symposium on building trust and confidence in the voting systems last December. Over 300 attendees from the election community were at the seminar to begin discussion, collaboration, and consensus building on voting reform issues.

Mr. Chairman, at this time, I would like to enter a copy of the CDs that contain the video transcripts of the symposium into the record. Thank you.

Chairman EHLERS. Without objection, so ordered.

Dr. SEMERJIAN. As required under HAVA, NIST recently delivered to the EAC a report which assesses the areas of human factors research and human-machine interaction, which feasibly could be applied to voting products and systems design to ensure the usability and accuracy of voting products and systems. The EAC delivered the report to Congress on April 30 of this year. Again, the specific recommendations of the report are included in my written testimony.

NIST views as a top priority accomplishing its responsibilities mandated in the HAVA legislation, in partnership with the EAC. These mandates include the recommendation of voluntary voting system standards to the EAC through its Technical Guidelines Development Committee. The first set of voluntary standards is due nine months after the appointment of the 14 members by the EAC. Last week, the EAC announced the membership of the TGDC, and their first meeting has been scheduled for July 9.

Under HAVA, NIST is directed to offer formal accreditation to laboratories that test voting system hardware and software for conformance to the current voting system standards. Yesterday, NIST announced in the *Federal Register* the establishment of a laboratory accreditation program for voting systems. NIST will carry out the accreditation of these laboratories through the National Voluntary Laboratory Accreditation Program, otherwise known as NVLAP, which is administered by NIST.

NVLAP is a long-established laboratory accreditation program that is recognized both nationally and internationally. NVLAP will also conduct a public workshop with interested laboratories in the near future to review its accreditation criteria, as well as receive comments and feedback from the participating laboratories and other interested parties. After the workshop, NVLAP will finalize specific technical criteria for testing laboratories and make the necessary logistical arrangements to begin the actual assessment of the laboratories. It is our intention that laboratories will be able to formally apply to NVLAP and initiate the assessment process in early 2005, if not sooner.

Laboratories seeking accreditation to test voting system hardware and software will be required to meet the NVLAP criteria for accreditation, which include the ISO/IEC 17025 standard, the 2002 Voting System Standards, and any other criteria deemed necessary by the Election Assistance Commission. To ensure continued compliance, all NVLAP accredited laboratories will undergo an onsite assessment before initial accreditation, during the first renewal year, and every two years thereafter to evaluate their ongoing compliance with specific accreditation criteria.

Only after a laboratory has met all NVLAP criteria for accreditation will it be presented to the EAC for its approval to test voting systems. The EAC may impose requirements on the laboratories in addition to the NVLAP accreditation.

Finally, NIST has compiled best security practices relevant to election security from current Federal Information Processing

Standards, FIPS. These standards are available on both the NIST web site and the EAC web site. This compilation is intended to help State and local election officials with their efforts to better secure voting equipment before the November 2004 election.

NIST realizes how important it is for voters to have trust and confidence in voting systems even as new technologies are introduced. Increasingly, computer technology touches all aspects of the voting process, voter registration, vote recording, and vote tallying. NIST believes that rigorous standards, guidelines, and testing procedures will enable U.S. industry to produce products that are high quality, reliable, interoperable, and secure, thus enabling the trust and confidence that citizens require, and at the same time, preserving room for innovation and change.

Mr. Chairman, thank you for the opportunity to testify, and I will be happy to answer any questions.

[The prepared statement of Dr. Semerjian follows:]

PREPARED STATEMENT OF HRATCH G. SEMERJIAN

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on NIST's responsibilities under the Help America Vote Act, specifically testing and certification of voting equipment. Major changes are taking place in the way we conduct elections. Our trusty old ballot boxes often are being replaced by a host of new technologies. Citizens are now much more likely to encounter optical scanners or touch screen systems at the polling place than a wooden box with a sturdy lock. As a result of these changes, Congress enacted the Help America Vote Act, commonly known as HAVA, and mandated specific research and development roles for the National Institute of Standards and Technology (NIST).

Many of the issues we are examining today are all directly related to standards and guidelines. As we like to say at NIST, if you have a good standard, you can have a good specification, and with proper testing you will be assured that the equipment performs as required. Congress understood the importance of standards in voting technologies and specifically gave the Director of NIST the responsibility of chairing the Technical Guidelines Development Committee (TGDC), a committee reporting to the EAC under HAVA. This committee is charged with making recommendations to the Election Assistance Commission (EAC) with regard to voluntary standards and guidelines for election-related technologies that have an impact on many of the issues we are discussing.

While we have considerable experience in "standards development," NIST understands that as a non-regulatory agency our role is limited and has started to meet with members of the "elections community,"—ranging from disability advocacy groups, voting advocacy groups, researchers, State and local election officials, and vendors—to learn about their concerns. Ultimately, in coordination with the EAC and the broader "elections community" we want to apply our "standards development" experience to election-related technologies so that, when voting is complete, the vote tally will be accurate and done in a timely manner.

NIST is by no means a newcomer to the issues related to electronic voting. Previous to the HAVA, NIST's involvement in studying voting machine technology resulted in the publication of two technical papers in 1975 and 1988. NIST's recent activities related to voting system technology have been preparatory to the implementation of HAVA and fulfilling the initial mandates of the law.

At the request of Congress and the National Association of State Election Directors, NIST organized and hosted a *Symposium on Building Trust and Confidence in Voting Systems* in December of 2003 at its Gaithersburg headquarters. Over three hundred attendees from the election community attended the seminar to begin discussion, collaboration and consensus on voting reform issues. Symposium participants included State and local election officials; vendors of voting equipment and systems, academic researchers; representatives of the cyber security and privacy community; representatives from the disability community, standards organizations and independent testing authorities, as well as newly appointed U.S. Election Assistance Commissioners. Representative stakeholders participated with NIST scientists in panels addressing:

- Testability, Accreditation and Qualification in Voting Systems;

- Security and Openness in Voting Systems; and
- Usability and Accessibility in Voting Systems.

Attendees agreed that they all shared the goals of:

- Practical, secure elections, with every vote being important;
- The importance of looking at the voting system end-to-end;
- The need for good procedures & best practices in physical & cyber security;
- The need to improve current testing & certification procedures;
- The need to separately address both short-term and long-term challenges; and
- The benefits of the election community working as a team.

As required under HAVA, NIST recently delivered to the EAC a report "which assesses the areas of human factors research and human-machine interaction, which feasibly could be applied to voting products and systems design to ensure the usability of and accuracy of voting products and systems, including methods to improve access for individuals with disabilities (including blindness) and individuals with limited proficiency in the English Language and to reduce voter error and the number of spoiled ballots in elections." The EAC delivered the report to Congress on April 30, 2004.

The report titled "Improving the Usability and Accessibility of Voting Systems and Products," assesses human factors issues related to the process of a voter casting a ballot as he or she intends. The report's most important recommendation is for the development of a set of usability standards for voting systems that are performance-based. Performance-based standards address results rather than equipment design. Such standards would leave voting machine vendors free to develop a variety of innovative products if their systems work well from a usability and accessibility standpoint. Additionally, the report emphasizes developing the standards in a way that would allow independent testing laboratories to test systems to see if they conform to the usability standards. The labs would employ objective tests to decide if a particular product met the standards.

In total the report makes 10 recommendations to help make voting systems and products simpler to use, more accurate and easily available to all individuals—including those with disabilities, language issues and other impediments to participating in an election. The recommendations highlight the need to:

1) Develop voting system standards for usability that are performance-based, relatively independent of the voting technology, and specific (i.e., precise).
2) Specify the complete set of user-related functional requirements for voting products in the voting system standards.
3) Avoid low-level design specifications and very general specifications for usability.
4) Build a foundation of applied research for voting systems and products to support the development of usability and accessibility standards.
5) To address the removal of barriers to accessibility, the requirements developed by the Access Board, the current VSS (Voting System Standards), and the draft IEEE (Institute of Electrical and Electronics Engineers) standards should be reviewed, tested, and tailored to voting systems and then considered for adoption as updated VSS standards. The feasibility of addressing both self-contained, closed products and open architecture products should also be considered.
6) Develop ballot design guidelines based on the most recent research and experience of the visual design communities, specifically for use by election officials and in ballot design software.
7) Develop a set of guidelines for facility and equipment layout; develop a set of design and usability testing guidelines for vendor- and State-supplied documentation and training materials.
8) Encourage vendors to incorporate a user-centered design approach into their product design and development cycles including formative (diagnostic) usability testing as part of product development.
9) Develop a uniform set of procedures for testing the conformance of voting products against the applicable accessibility requirements.
10) Develop a valid, reliable, repeatable, and reproducible process for usability conformance testing of voting products against the standards described in recommendation 1) with agreed upon usability pass/fail requirements.

NIST views as a top priority accomplishing its impending responsibilities mandated in the HAVA in partnership with the EAC. These mandates include the recommendation of voluntary voting system standards to the EAC through its Technical Guidelines Development Committee. The first set of voluntary standards is due nine months after the appointment of the fourteen members by the EAC. Last week the EAC announced the membership of the TGDC. The first meeting of the TGDC has been scheduled for July 9, 2004.

Under HAVA, NIST is directed to offer formal accreditation to laboratories that test voting system hardware and software for conformance to the current Voting System Standards. This week, NIST is announcing in the *Federal Register* the establishment of a Laboratory Accreditation Program for Voting Systems. NIST will carry out the accreditation of these laboratories through the National Voluntary Laboratory Accreditation Program (NVLAP), which is administered by NIST. NVLAP is a long-established laboratory accreditation program that is recognized both nationally and internationally. NVLAP accreditation criteria are codified in the Code of Federal Regulations (CFR, Title 15, Part 285).

NVLAP will conduct a public workshop with interested laboratories in the near future to review its accreditation criteria, as well as receive comments and feedback from the participating laboratories and other interested parties. After the workshop, NVLAP will finalize specific technical criteria for testing laboratories and make the necessary logistical arrangements to begin the actual assessment of the laboratories. NVLAP must identify, contract, and train technical expert assessors; laboratories must complete the NVLAP application process; rigorous on-site assessments must be conducted; and laboratories undergoing assessment must resolve any identified non-conformities before accreditation can be granted. It is our intention that laboratories will be able to formally apply to NVLAP and initiate the assessment process in early 2005 if not sooner.

Simply stated, laboratory accreditation is formal recognition that a laboratory is competent to carry out specific tests. Expert technical assessors conduct a thorough evaluation of all aspects of laboratory operation that affect the production of test data, using recognized criteria and procedures. General criteria are based on the international standard ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories,* which is used for evaluating laboratories throughout the world. Laboratory accreditation bodies use this standard specifically to assess factors relevant to a laboratory's ability to produce precise, accurate test data, including the technical competency of staff, validity and appropriateness of test methods, testing and quality assurance of test and calibration data. Laboratory accreditation programs usually also specify field-specific technical criteria that laboratories must meet, in addition to demonstrating general technical competence.

Laboratory accreditation thus provides a means of evaluating the competence of laboratories to perform specific types of testing, measurement and calibration. It also allows a laboratory to determine whether it is performing its work correctly and to appropriate standards.

Laboratories seeking accreditation to test voting system hardware and software will be required to meet the NVLAP criteria for accreditation which include: ISO/IEC 17025, the 2002 Voting System Standards, and any other criteria deemed necessary by the Election Assistance Commission (EAC). To ensure continued compliance, all NVLAP-accredited laboratories undergo an on-site assessment before initial accreditation, during the first renewal year, and every two years thereafter to evaluate their ongoing compliance with specific accreditation criteria.

Only after a laboratory has met all NVLAP criteria for accreditation will it be presented to the Election Assistance Commission for its approval to test voting systems. The EAC may impose requirements on the laboratories in addition to NVLAP accreditation.

Finally, NIST has compiled best security practices relevant to election security from current Federal Information Processing standards (FIPS). These standards are available on the NIST web site *(http://vote.nist.gov/securityrisk.pdf)* and will be available on EAC's web site *(http://www.fec.gov/pages/vssfinal/vss.html).* This compilation is intended to help State and local election officials with their efforts to better secure voting equipment before the November 2004 election.

NIST realizes how important it is for voters to have trust and confidence in voting systems even as new technologies are introduced. Increasingly, computer technology touches all aspects of the voting process—voter registration, vote recording, and vote tallying. NIST believes that rigorous standards, guidelines, and testing procedures will enable U.S. industry to produce products that are high quality, reliable, interoperable, and secure thus enabling the trust and confidence that citizens require and at the same time preserving room for innovation and change.

Thank you for the opportunity to testify. I would be happy to answer any questions the Committee might have.

BIOGRAPHY FOR HRATCH G. SEMERJIAN

Hratch G. Semerjian is serving as Acting Director of NIST while Arden Bement serves in a temporary capacity as the Acting Director of the National Science Foundation. Dr. Semerjian has served as the Deputy Director of NIST since July 2003. In this position, Dr. Semerjian is responsible for overall operation of the Institute, effectiveness of NIST's technical programs, and for interactions with international organizations. NIST has a total budget of about $771 million, and a permanent staff of about 3,000, as well as about 1,600 guest researchers from industry, academia, and other national metrology institutes from more than 40 countries. Most of the NIST researchers are located in two major campuses in Gaithersburg, Md., and Boulder, Colo. NIST also has two joint research institutes; the oldest of these is JILA, a collaborative research program with the University of Colorado at Boulder, and the other is CARB (Center for Advanced Research in Biotechnology), a partnership with the University of Maryland Biotechnology Institute.

Dr. Semerjian received his M.Sc. (1968) and Ph.D. (1972) degrees in engineering from Brown University. He served as a lecturer and post doctoral research fellow in the Chemistry Department at the University of Toronto. He then joined the research staff of Pratt & Whitney Aircraft Division of United Technologies Corp. in East Hartford, Conn. In 1977, Dr. Semerjian joined the National Bureau of Standards (now NIST), where he served as Director of the Chemical Science and Technology Laboratory (CSTL) from April 1992 through July 2003. Awards he has received include the Fulbright Fellowship, C.B. Keen Fellowship at Brown, the U.S. Department of Commerce Meritorious Federal Service (Silver Medal) Award in 1984, and the U.S. Department of Commerce Distinguished Achievement in Federal Service (Gold Medal) Award in 1995. In 1996, he was elected a Fellow of the American Society of Mechanical Engineers. In 1997, he received the Brown Engineering Alumni Medal. Dr. Semerjian was elected to the National Academy of Engineering in 2000.

DISCUSSION

Chairman EHLERS. Thank you very much, and thank all of you for your testimony. We will now begin with the questioning, and I yield myself five minutes for that purpose.

ELECTION MANAGEMENT BEST PRACTICES AND ACCEPTANCE TESTING OF VOTING EQUIPMENT

A couple of things, first of all. We are concerned about the initial testing of the equipment and the software. We want to make sure that it meets the design criteria, specifications, that it works as it is intended to work. The second aspect is to preserve that as time goes on, and ensure that it continues to operate properly. Let me just, for my own information, ask a question about that. Perhaps Mr. Wilkey would be the one to answer. Others may want to comment.

On the newer electronic machines, do the manufacturers provide some type of self-test routine that you run the computers through before each election? In other words, you insert this in, it runs through, checks the software, and makes sure it is doing what it is supposed to do, that no one has tinkered with it? Is that standard or is that just not done at all?

Mr. WILKEY. Mr. Chairman, thank you for asking that question, because it gives me an opportunity to talk about something that I have been on my soapbox for over 15 years, and now, as a private citizen, it may be the last time I have a chance to talk about it publicly.

Certainly, what we have tried to do in the area of standards development and testing of an initial product is only 50 percent of the battle.

Chairman EHLERS. Yeah.

Mr. WILKEY. The next 50 percent, and perhaps even the most important part of what we are talking about, is what needs to happen once the product is delivered to the jurisdiction. And that is where we have consistently talked about doing acceptance testing of a quality that is developed by the jurisdiction and not the vendor, is done by the jurisdiction and not the vendor, and similarly, all of the maintenance activities and the pre-election testing that must occur, ongoing, throughout the process.

One of our biggest problems in election administration in this country is that there are over 13,000 election jurisdictions. Many of them, as you know, Mr. Chairman, in your own State, and in mine, are very small. They are mom and pop operations with the county clerk that may have a number of responsibilities, or a town clerk, if you are talking about the New England states. They don't have the expertise always available to them to do this, so on many occasions, they are relying on the vendor to do this.

This is a practice that we are trying to stop, and what we are hopeful, with the new Election Assistance Commission, that they will get the necessary funding to be able to do what I have talked about for the last 15 years, and that is the management operational standards, that—it is a huge project. But it needs to be done, because jurisdictions need to be able to go some place to say I have bought this system. This is how I do an adequate test. This is how I develop the test. This is how I do ongoing maintenance. This is the kind of maintenance logs I have to keep, and on and on and on. Because it is only that 50 percent of the battle that we are seeing in the news media today.

And another part of our problem, which I think the EAC hopefully will address, and which the Chairman has addressed already in his remarks a couple of weeks ago, is that we keep hearing there are problems out there across America with these systems. One of the things that we are not able to determine is how many of these units are out there, and how many of these units have problems, and what are these problems?

Hopefully, and the Chairman of the Commission, Chairman Soaries, has called on every election jurisdiction in the country to report to the EAC the problems that they are having with their equipment, so that we can begin to see what is going on, and we can see a pattern, and that the TGDC can begin to take a look at the problems, then, and try to prevent them from happening in the future.

So, thank you, Mr. Chairman. I am glad you asked that question.

Chairman EHLERS. Well——

Mr. WILKEY. Because it is very important.

Chairman EHLERS. And my point simply was, it seems to me because there are a lot of mom and pop operations, and I am very familiar with that, that we should expect the manufacturers to provide the testing software and materials to test—at least test the software that is on the machine. The county clerk or the township clerk can do—can set up 10 machines and run a quick fake election

with employees, and make sure that it works, to really make sure it hasn't been tinkered with.

Mr. WILKEY. Yes, I agree, Mr. Chairman, and one of the things we encourage everybody to do, one of the projects that is going on right now at the EAC, and which I have been involved in, is to do a series of best practices that will be out and available to election jurisdictions over the next several weeks.

And through this project, jurisdictions will be able to go to the EAC web site and take a look at some examples of tests that should be done on various equipment. I think it is good for the vendor to provide this information to the jurisdiction, but I think the jurisdiction has to go beyond that.

Chairman EHLERS. Yeah.

Mr. WILKEY. And so if a vendor says you have got to test this, this, and this, the jurisdiction should be taking and say yes, we are going to test this, this, and this, but we are going to do it four times.

Chairman EHLERS. Dr. Shamos, I thought I saw you indicating a twitch when I asked the question.

Dr. SHAMOS. Yes, you did, Mr. Chairman.

The processes that we are talking about here are much more out of control than anyone is willing to admit. There are essentially no controls on how software enters a voting machine these days.

We know how it gets there when the machine is sold. However, it is often necessary for the vendor to fix bugs, add new features, make customizations that are specifically requested by the jurisdiction. There may be statutes that require them to submit that software for recertification, but there is nothing that physically prevents them from putting a chip into a FedEx envelope and sending it directly to the county clerk, with instructions to install this chip, whose contents they have no knowledge of, into a voting machine.

And the problem, of course, is exacerbated by the fact that we have over 3,100 counties in the country, so essentially, 3,100 different elections, and that is another place where the degree of sophistication or lack of it comes into play. They are simply not equipped to know what to do to test this new thing. Now, the idea that the vendor would be able to supply testing software whose specific purpose is to reveal flaws in the activities of the vendor doesn't seem to be a stable situation to me.

There are certain kinds of tests that one naturally performs, is the processor operating? Are the lights on the panel operating, et cetera. But if the allegation that has been made by security specialists is rational, that a vendor could himself introduce malicious code, or code designed to influence the outcome of an election, then we certainly can't rely on the vendor's testing protocols to reveal that.

And so, I believe there have to be nationwide standards that apply, otherwise we are going to run into an equal protection issue, that a voter in one state will not be accorded the same degree of—literal protection against having his vote tampered with than a voter in another state.

Chairman EHLERS. Ms. Coggins.

Ms. COGGINS. I would concur.

Currently, the voting system standards do actually have an operational test that must be performed, and the labs have to test for that. But at this point, there is no standard that tells a jurisdiction how do you go and do this validation? How can you check to see that the code you have matches the code that was qualified by the lab, or is certified by your state?

I would suggest that actually, as Dr. Shamos has added that into the standards. The whole process is jurisdictions are not exempt from audit, and that audit is not—just because the voting system has been tested, it doesn't mean that you still don't have to run the same kind of manual audits that you ran against your registration system.

It is not yes, you have a computer system, but you know, test, but verify. I mean, that is—trust, but verify, sorry.

Chairman EHLERS. And test, as well.

Ms. COGGINS. Yeah. That is right. And also, just in terms of the clearinghouse role, you know, that was part of the original intent of the 1990 implementation plan, that there was a clearinghouse where all of this information could be reported back on, on this anecdotal information. If the EAC could somehow have a reporting mechanism, where you can go online and you can, as a local jurisdiction, you can type into a database, and the form is set up in a way that it is—a software reporting, defect reporting, something along those lines, where it is structured, where you can really guide people, okay, here is the information we need you to get. I would also suggest that, in terms of the overall end-to-end process of education for elections, you look at putting something out there that can help local jurisdictions report back to this clearinghouse.

Chairman EHLERS. Thank you all, and I—my time has expired. I will now yield to the gentleman from Colorado, Mr. Udall.

Mr. UDALL. Thank you, Mr. Chairman. I want to thank the panel as I begin. It was very helpful. As you all know, I think you raised more questions than you answered, but that is the purpose of having a hearing.

SHOULD ALL COMPUTER-BASED VOTING EQUIPMENT BE REQUIRED TO HAVE A PAPER TRAIL?

If I could direct a question to Dr. Shamos, I think this maybe gets at one of the questions we all ask ourselves, particularly given what Congressman Holt had to say. There are a number of computer experts that strongly recommend that all computer-based equipment have a paper ballot trail. You alluded to this. Congressman Holt alluded to it.

What are your views on this recommendation?

Dr. SHAMOS. Congressman, there are already requirements in place for DRE machines in certain states to have paper audit trails. These are not the so-called voter verifiable audit trails, but they are a continuous roll of paper that records a complete ballot image of every vote cast, and in fact, I haven't recommended certification of any DRE system that didn't possess such a capability.

We are talking about the voter verified paper trail, the one that produces a piece of paper that the voter may see, so that he can verify that his vote has—corresponds to the buttons that were pressed, or whatever actions had to be taken. And the idea is that

that voter verified ballot is not taken away from the voting booth with the voter, but is deposited in a secure receptacle within the machine, so it is available for some process later on, whether that is an audit, or a recount, or some other activity associated with an election contest.

I don't have anything against paper in general. The problem that I have with those proposals, and particularly, that single sentence in Representative Holt's bill, is the sentence that says that the paper record shall be the official one, and that it shall take precedence over the electronic record. The reason I take issue with it is that this country has a very long and sorry history of vote tampering, and that vote tampering has almost exclusively been conducted through the use of physical ballots, whether they were ordinary paper ballots, punched cards, mark-sense, or otherwise.

The *New York Times,* which has recently been so fond of supporting the concept of a paper trail, has published over 4,700 articles during its history on vote tampering around the United States with paper ballots. And those 4,700 articles date back to 1852, and if you do the division, it is that the *New York Times* has published such an article on an average once every 12 days since it began publishing in 1851, it has decried the use of paper ballots as a way of recording votes. Yet in 2004, when nothing had changed, the *New York Times* decided suddenly that paper was the right mechanism.

What has not occurred here, and what the computer specialists who recommend paper trails have not done, is to do a security comparison between the security vulnerabilities of DRE systems and the security vulnerabilities of paper. If, on balance, paper is safer, then that is the system we should be using. But it is the reason we don't use paper. The Kolth, or lever machines, beginning in the 1890's, which led in 1925 to New York adopting lever machines, was specifically to combat chicanery with paper ballots.

So once the paper ballot becomes the official one, anybody who has any mechanical capability at all is able to fiddle with paper ballots, but they can't fiddle with properly secured cryptographically encoded electronic records. That is why I am not in favor of them becoming official.

Mr. UDALL. You may be very popular around here, because there are certainly a lot of people who look for instances in which the New York Times contradicts itself.

Chairman EHLERS. They are not that hard to find, actually.

Mr. UDALL. So in effect, you are saying there are those that hear all of the arguments about DREs and the problems who might say why don't we just say to ourselves, look, technology isn't the answer to everything. Let us just go back to paper ballots, because they are verifiable. They are in your hand. There is no hidden software, but you point out that that, although on the surface, may seem like a viable option, it has its own problems, and fraught with its own history.

Dr. SHAMOS. I have asked those experts personally. I said tell me, make a list of problems that you believe that paper trails are intended to solve, and then demonstrate to me the way in which the paper trail solves the problem, and they are unable to do it with a single exception, and I will give them this, that when the

voter goes into the voting booth, she wants to be sure that her choices have been properly understood by the machine. She needs some feedback that says that. The paper, the piece of paper does, indeed, provide that feedback. There are numerous other ways of providing it that are completely electronic, but the paper does it. The fallacy is in believing that once that piece of paper is cut off and drops into a receptacle, that it will be around for a recount, that it will not have been modified. It will not have been deleted. It will not have been augmented. There is no, absolutely no assurance that those things will not happen. So, they solve, of the top 10 problems with DREs, it is possible that paper trails solve one.

Mr. UDALL. I see my time has expired. I do fall back to some extent on an ATM analogy. I know, at least it is my habit. I deposit some money, or I remove some money, and I get a little paper receipt, and I stick it in my wallet, and carry it along with me, and sometimes I check, and sometimes I don't, to see if that it is, in fact, what has been recorded in my savings or checking account.

Dr. SHAMOS. Well, I am glad you raised that analogy, because if you read Reg E of the Federal Reserve Board, which requires such paper receipts from ATMs, you will find that the paper receipt is not the official record of the transaction. All it is is a piece of evidence, and if there is a discrepancy between the electronic record and the piece of paper, that is the starting point for the bank's investigation. It is not the endpoint, and I believe it should be exactly the same with voting systems. If there is a discrepancy between the paper audit trail and the electronic record, that is where we start looking, and we do a forensic examination to see who did the tampering. We don't simply take the paper record and say, that is it. We don't have to look at the electronics any more, because all that means is we are simply returning to hand-counted paper ballots.

Mr. UDALL. Thank you.

Chairman EHLERS. If I may just interject here, I assume you would agree with my statement to Mr. Holt that it would not be too much trouble to program the computer to store one record that is different from the one that is printed out.

Dr. SHAMOS. Oh, one can certainly program a computer to do that.

Chairman EHLERS. Yes.

Dr. SHAMOS. However, I don't agree that it would be possible to do that in such a way that it would not be detected during testing, qualification——

Chairman EHLERS. Yes. Yes. Right. I agree. Next, I am pleased to yield to Mr. Gutknecht, my friend from Minnesota.

Mr. GUTKNECHT. Well, thank you, Mr. Chairman, and I want to thank the distinguished panel today. I appreciate the testimony.

I am still sort of torn on this whole issue, because I guess there are sins of omission, there are sins of commission, and I am not sure how many problems we have with various voting machines, but I do believe we in the United States and, frankly, even in my own State, on occasion, have problems with people who would try to alter the outcome.

In fact, in my own district, we had a very disputed State senate election last time. We—and it was paper ballots, and you could say

we had an audit trail, and in one of the most disputed precincts, one of the election judges inexplicably took a bunch of ballots home and burned them in her fireplace.

Dr. SHAMOS. It must have been cold.

TECHNOLOGIES FOR REDUCING VOTER FRAUD

Mr. GUTKNECHT. It was cold. It was Minnesota, and it was November, December, by the time they got to this. But I guess what I really, and maybe this is a question for the folks from NIST. It seems to me if we are going to get serious about really cleaning up the elections, we have to do something to make certain that the people who are actually voting are the people that say that they are. In other words, most of the examples, I think, where we have had what I would describe as voter fraud is where people who were not eligible to vote voted, and where people may have voted in more than one precinct, and unfortunately, I think that has been happening more than most people would like to admit.

And so far, we have talked an awful lot today about, you know, voting machines and making certain that they tabulate correctly, and that the voters' wishes are expressed, but I guess the question I would have is how do you ultimately, as Mark Twain once observed, you know, we as politician's are America's only native criminal class, and so there is always this temptation to figure out ways to tweak the system to somebody's advantage, and I really have been less concerned about the tabulation by the machine than I have what some of the political machines might do to try and change the outcome illegally.

And have you worked at all on trying to tie those ends together?

Dr. SEMERJIAN. We have not, so far, but I think that will be probably one of the major agenda items for the TGDC, in terms of how do you assure that the person who presents himself or herself there is the person, and then, how do you—I mean, we have a lot of different technologies.

Mr. GUTKNECHT. Right.

Dr. SEMERJIAN. Some of them are being used today, with you know, some of the magnetic cards that they give you, based on your presentation of an ID, so I think the technologies are there. The issue is how are they implemented locally, and a lot of the uncertainties probably come from local implementation of these issues. So, frankly, TGDC and the EAC can provide guidelines, standards, for all those issues, but these are, after all, voluntary standards. They will be voluntary standards, so it will be up to the local jurisdictions to decide how far they go.

Mr. GUTKNECHT. Well, I thought for a long time, there ought to be a way that when someone votes, that they leave a fingerprint, and the technology is relatively simple on biometrics. I mean, I say that relatively, but—and more importantly, it is not that expensive nowadays to really confirm that, you know, that person is who they say they are, but more importantly, that they haven't voted anywhere else that day. And I really think that NIST could be helpful in perhaps bringing some of that technology together, and at least demonstrating to local election officials that this is available now, and yes, we could do all we can to make certain that the technology that we are using is accurate, but at the end of the day, you know,

the other side of that equation is we have got to make certain that the people who are voting are eligible to vote, and that they haven't voted more than once.

Dr. SEMERJIAN. Well, I wouldn't have agreed with you three years ago, but today, certainly, the technology is there, because of the visa, you know, entry, and that technology is certainly available. But there are, of course, philosophical issues. Not everybody is—we don't have everybody's fingerprint, and how would that be accepted in the community as a whole? And whether the costs of implementing a system like that in all of the jurisdictions would be acceptable.

I don't think that is a technology issue.

Mr. GUTKNECHT. Correct.

Dr. SEMERJIAN. I think it is an implementation issue, cost issue, and some philosophical issues, whether we will require the whole country to have, basically, a fingerprint of every eligible voter.

Mr. GUTKNECHT. Well, I think if we wait until we have a complete consensus, we will never move on any kind of a universal system, so that we do have that kind of technological guarantee. And that is where I think NIST can play an important role, as we begin to say to communities and States, look, this stuff exists, and it can be integrated. Now, it may not happen overnight, but if you don't start today, you will never get there. And I really think that is a very important part of this story, that you know, I am not as worried about the machines that we use in Minnesota not counting correctly, as I am about large numbers of people in some precincts that maybe half a dozen people or a dozen that could change the outcome of a school board election, or a State legislative election, or even a Congressional election.

And so, I do hope that as you go forward, you will at least keep open to that, and try to at least let folks know that this technology is out there. It is not all that expensive. I think the concern I have with, you know, with your immediately going to the philosophical question. You may well be right. But I think generally speaking, the public has always resisted new technologies. I mean, there were people who thought putting electrification inside of houses was ludicrous because people would die. And of course, they were right. I mean, people have died from being electrocuted. But, you know, we figured out that it is a risk we are willing to take, and we take it every day. And I think that is going to be true with this technology. I think at first, there will be resistance, but more and more people realize it is for their protection as well.

I yield back the balance of my time. Thank you.

ROLE AND ABILITY OF NIST TO ADDRESS VOTER EQUIPMENT TESTING AND EVALUATION ISSUES

Chairman EHLERS. The gentleman's time has expired. I will ask some additional questions. And let me just interject here, in the midst of all this gloom and doom about fraud, error, and so forth, that I am pleased that we live in a country that, by and large, values the integrity of their elections, and the majority of the people, in fact, are honest and want honest elections.

So, it is not all bad news, but the point is, we want to protect it and make sure that people can be assured, first of all, that their

vote counts, and secondly, that there are no fraudulent votes counted, and that all votes are counted accurately.

This is a question for anyone on the panel. How important is NIST's role at this point in solving the problems we have discussed here today? What specific assistance do you need from NIST, or do you think NIST should provide, both what they already are doing, and what they might potentially do? And then I would like to ask NIST to respond whether or not they can meet these needs, and how much funding would be required.

Mr. Wilkey, we will start with you.

Mr. WILKEY. Thank you, Mr. Chairman.

One of the issues that the Chairman of the EAC has come out with in the last couple of weeks—I mentioned them earlier—he has called on—and I know that he has personally called every one of the vendors, and asked them to voluntarily place their software and source code into the NIST software library—and this is something that we had been talking about in all of our discussions, going back a year ago, that one of the great benefits that NIST brings to this whole program is to be able to have a single repository for software source code, all of the versions, because there are so many versions out there. It is one of the most difficult things that we have to deal with, or that the ITAs have to deal with, is version control. And to bring them into this library, similar to the one that they host now for the law enforcement agencies all over the country, would be a great benefit to this program.

Let me just interject also, and I may have mentioned this before, but I—we came away from our initial meetings with NIST so gratified that the little baby that we tried to raise is now kind of grown up, and we can turn it over to them, and feel confident that they are going to give it the day to day attention that it really needs.

We were particularly gratified because NIST, and we didn't know this before we began meeting with them, is that NIST has the ability, being who they are, to bring the very best in technology to the table to look at these issues, and to study these issues, and to make the very best recommendations that they can. And so, we are very pleased from our end, and as non-technical people. I am not a technician, never claimed to be. I am just a school teacher who ended up going into the Election Office 35 years ago, and here I am today.

But I think all of us in NASED who have been working on this have particularly been very much pleased with what we have seen at NIST, and we know that they will do a great job in this area.

Chairman EHLERS. Well, let me just thank you for that statement, because you have no idea how many objections I received from members of your organization when I first proposed NIST.

Mr. WILKEY. Chairman, we were a little skeptical, but we were quick learners. Let us put it that way.

Chairman EHLERS. More than a little skeptical. Ms. Coggins, do you have any comment on the question of how important NIST is, and what the appropriate role is?

Ms. COGGINS. I think I would just say that a reexamination of the voting system standards is appropriate, and we definitely support, you know, any help that can be provided by NIST. I think,

you know, it is good to have an organization such as them helping with that process.

Chairman EHLERS. Okay. Dr. Shamos, any comment?

Dr. SHAMOS. Yes, Mr. Chairman.

I think the nature of voting system standards, they differ from other kinds of standards. The Chair mentioned we have Underwriters Laboratories testing of various electrical devices, so we believe we are safe from shock. But if half the people who use toasters got electrocuted, we would look very carefully at what Underwriters Laboratories was doing.

So most people in their daily life do not need to understand the testing procedures or even the standards that are being applied to toasters, because our experience is that they are safe. However, so much hue and cry has been raised about security problems and reliability problems with voting systems that I do not believe that the public will be satisfied with standards that the public cannot observe and understand.

And therefore, I think that the proper role of NIST is to coordinate the development of standards with massive input from the public, and massive transparency and visibility, similar to the way Internet standards are developed, by having Requests for Comment, engineers all over the world look at the protocols, make comments, and what happens is that the cream rises. And if someone has an idea that is bad, there are 100 people who explain why it is bad.

Instead of looking to a super-organization who, essentially, takes on the mantle of we are the experts, trust us. The word trust is rapidly disappearing from the process of voting and counting votes. We can just never get the public to buy the concept that some distinguished gentleman ought to be trusted simply because they have been around a long time. And we need much more public involvement.

WHAT DOES NIST NEED TO FULFILL THIS ROLE?

Chairman EHLERS. Thank you. And to wrap this up, Dr. Semerjian, two questions. Can NIST meet these needs? How much funding will it require? And HAVA gave you nine months to develop a standard. Can you meet that deadline?

Dr. SEMERJIAN. First of all, we are very pleased to be involved in this. Our mode of operation has always been to be open and transparent in anything. We don't have many smoke-filled backrooms where things get decided. Indeed, the standards setting process, everything that we do is open, through the normal procedure of publishing notices in the *Federal Register,* giving sufficient time to people to comment, or almost invariably, having workshops to not only welcome, but indeed solicit comments from the public, and the technical community.

So, I certainly have no reservations in terms of meeting the kinds of requirements that Dr. Shamos has in mind. I mean, indeed, this is an area where public trust and confidence, just the perception, is a very important issue. The fact that scientists or engineers can sit and convince each other that this works or this is right is not sufficient. The process has to be open enough, transparent enough, so that everybody understands, as he pointed out.

So, it is very important, and indeed, our process of doing any of these kind of activities, have been along these lines. And we don't normally just sit and decide on one particular standard. As you know, in the encryption standards, for example, we opened the field to the whole world, basically asked scientists, engineers, to come with proposals for the kinds of standards that we should have. So, I expect a similar process. I think our only problem will be we are running on such a short time scale that——

Chairman EHLERS. And that was a question.

Dr. SEMERJIAN. Yeah.

Chairman EHLERS. Can you meet the time?

Dr. SEMERJIAN. I think so. But it will—I mean, we already have the—as I pointed out, we have put—the *Federal Register* notice came out yesterday. We expect the workshop within a month or so, and we will certainly give our best try to meet the nine-month deadline to come up with a draft standard.

Chairman EHLERS. And the funding?

Dr. SEMERJIAN. Well, I guess that is really hard to say, but we will—I know you are working very hard to come up with resources for NIST, and we will try to get that done within——

Chairman EHLERS. Yeah. And as you know, I did try to take some of the funding that was for the new voting machines, and just divert a very small fraction of that to you, but received objections from NASED, for which I will never forgive them, and so that wasn't accomplished. But perhaps that can still be done.

Thank you. My time has expired. We are rejoined by the Ranking Member, Mr. Udall, if you have further questions.

Mr. UDALL. Thank you, Mr. Chairman.

I am glad to hear that NIST believes that you can get the job done. But I do think it is incumbent on us to provide you with the resources, and I hope you will continue to make that case, as will members of the panel, to the Congress. The squeaky wheel gets the oil is certainly a principle that works in the Congress.

I, Mr. Chairman, want to just for the record note that I talked to our Secretary of State, who I think may be familiar to some of the panel, Donetta Davidson, last week, and asked her some questions about what was unfolding in Colorado, and she is, Mr. Chairman, for the record, she is a moderate, thoughtful Republican.

Chairman EHLERS. All Republicans are moderate and thoughtful.

Mr. UDALL. Thoughtful at all times, I know. And a well-respected public servant, and her point was get NIST the resources, and get NIST on the case, and we can move to where we need to be, that the 2006 deadline is bearing down upon us, and that was her focus, not the 2004 election. I do fear that we may have the potential in 2004 for a repeat of 2000 at the Presidential election level, but be that as it may, we certainly have that 2006 deadline to meet.

Dr. SEMERJIAN. Mr. Udall.

Mr. UDALL. Yes.

Dr. SEMERJIAN. I don't know if you are aware of it, but Ms. Davidson is on the TGDC.

Mr. UDALL. Yes.

Dr. SEMERJIAN. She is a member of the TGDC, and we are very pleased to have that expertise on the Committee.

Mr. UDALL. She brings, of course, a county perspective, because she served in that role as the county clerk in Arapahoe county, which is a very populated county south of Denver, and now, she is the Secretary of State. And as I mentioned, highly respected by Members of all parties in Colorado.

WHAT DO STATES AND OTHER ENTITIES NEED TO DO TO IMPROVE THE TECHNOLOGICAL ASPECTS OF ELECTIONS?

I thought I might try and stir things up with my last question, because I think the answer to this will—I want to give everybody a chance, but I want to return to Dr. Shamos, and he raised a number of questions about the current standards and testing procedures, as well as some recommendations on how they could be improved, and I thought I would love to hear from each of the panel members, your views on Dr. Shamos' testimony in that regard. Let me start with Mr. Wilkey and move across.

Mr. WILKEY. Thank you for your comments about the Secretary of State, who is a very good personal friend of mine, and I have spent so much time in your State lately over the last year, I nearly meet the qualifications to be able to vote for you. So, if I defect, or——

Mr. UDALL. Mr. Gutknecht may want to get your fingerprints before you——

Mr. WILKEY. Okay.

Mr. UDALL [continuing]. You are allowed to vote.

Mr. WILKEY. While I appreciate Dr. Shamos' statements, I want to reiterate, as I did in my testimony, that we certainly have done the very best job we could do on a voluntary basis, not having any staff, not having any funding, but trying to keep it going for the benefit of our member States and our jurisdictions. Certainly, there are some areas that need to be addressed, and we are hopeful that the Technical Guidelines Development Committee, which will be having its first meeting in the next couple of weeks, will be able to address those.

Certainly, and I want to re-emphasize again the role the states and jurisdictions need to play in this process. You know, you can take a toaster, for example, as was already mentioned here, and you can put it in the lab, and you can test it, and you can, you know, similar to what we do with voting systems. You know, we put them in a chamber, and run them for 163 hours, and shake them and bake them. And you know, can come out with a clean bill of health, but if you don't do what is necessary at the local level, you have lost all of that, essentially, because you are only testing one unit. And so it is absolutely necessary that—and something that we have talked about in NASED for a long time, that our states have to take the bull by the horn in doing that, similar to what they are doing in your State, Congressman, in your State, Mr. Chairman, in some of the states that have put funding to adequately do this job, places like my own State, where we have a dedicated staff that does that. The State of Florida, State of California, Georgia, and others, that have seen the need to have their own people on staff to be able to continue to make that whole process work.

And so, I think that this is the most important thing that we need to understand in this whole process.

Mr. UDALL. Ms. Coggins.

Ms. COGGINS. Well, I think one of the points is that—and I don't take it that Dr. Shamos is saying that there is—the labs have an integrity problem at all. I am not interpreting it—it is a transparency problem, is part of his view. And we agree that there can be greater transparency in this process. You know, I think I keep going back to this 1990 implementation program.

One of the original issues in that was that the reports were supposed to be provided—the FEC was going to have this clearinghouse where they could distribute the reports to the states, and somehow, that didn't happen, and you wound up making the person who distributes the report someone who has a nondisclosure agreement. And so, at this point, whether or not a state gets a report or not, it depends upon the vendor to request the lab to send it. You know, I would say in terms of that, if the State and the local person don't request the report, the report remains confidential because they allow it to remain confidential.

But we agree that there can be greater transparency in the process. We have also tried to be, by coming here today, and other things that we do to support NASED, we have gone before the California taskforce. We went to the NIST conference. We try and get our processes out. Quite frankly, I start talking and eyes glaze over in one minute, when you start talking about test process. So, I know that there is an interest in greater participation, and we definitely feel that, you know, transparency, in terms of reports, in terms of the accreditation, we don't have an issue with that.

Mr. UDALL. Dr. Semerjian, I think maybe it is—I don't know if it is inappropriate for you to answer, but I know this is what—the area in which you are going to do some work. If you feel comfortable responding, I would welcome your input.

Dr. SEMERJIAN. No—I see no reason why reports should not be available, whether it is the accreditation report, or the test reports. The other comment, I thought Dr. Shamos was making, that you know, if people send you a chip, and you know, somebody can just plug it in, and that is perfectly okay, that is not an acceptable procedure under ISO 17025 standard. You can't just plug things in and take things out, make changes, without proper notification and proper documentation of those changes. So, I think just by implementing more rigorous test procedures and standards, I think we should be able to get over some of those difficulties.

I think his concern is well-placed, in the sense that we need to be worrying about not just a box, a piece of apparatus here. We need to—or just the chip inside. We need to worry about the integrity of the whole system, the whole system being first, the machine itself, and second, not just the voting machine, but how does that data get transmitted to a central location where the vote is tallied, etc.

So, clearly, our concerns have to be not just limited to one particular box, one particular element of the system, but the entirety of the system. I think clearly, we have to look at the totality of the systems that are being used.

Mr. UDALL. Spoken like the head of NIST. Thank you, and again, I want to thank the panel. I think we are going to conclude here. But what I heard, Dr. Shamos, you saying in the end, that this is more about human error than it is about fraud, although we always have to be worried about fraud. But that, in the end, that is more where you would place your concerns, given the multiplicity of systems around the country, and the difficulty in arranging some sort of a fraudulent conspiracy, if you will.

Dr. SHAMOS. Well, we must be thoroughly vigilant to make sure that the systems are not vulnerable to fraud. We shouldn't engage in the fantasy that electronic frauds are going on all the time, or that that is the major problem that we face in elections. Most of the incidents that I have read about involve machines that simply won't boot up properly on election day. That has nothing to do with fraud. What it has to do with is either people not knowing how to turn them on, or machines that have not been adequately tested, stored, or set up properly. That is an education problem.

But I am certainly not suggesting that security is not a vital concern.

Mr. UDALL. And thanks to the panel. This is very informative.

Chairman EHLERS. The gentleman's time has expired. Mr. Wilkey, did you have something you wanted to say? It looked like you wanted to make a comment.

Mr. WILKEY. And I would like to do just a quick followup on the question that Congressman Udall asked.

You know, we have often been accused of—because this was a voluntary effort of having a rinky-dink process here, this is the handbook that NASED uses to qualify our ITAs. When we move this process over to NIST, they will use a process called ISO 17025. It is a very familiar accreditation standards for independent test authorities. It is almost a carbon copy of the handbook that we have been using for a number of years, because it was developed when the first draft of 17025 was being drafted by the late Bob Naegele, who did all of this work, and who worked closely with NVLAP and NIST at that time.

Further, we have had some of our own questions regarding these reports. We have consistently told our member States that have been involved in this program, and believe me, it took a long time to get 41 states to adopt the voluntary federal standards, a lot of talking, and a lot of arm-twisting. But we finally did it, and one of the things that we have consistently told these states is that they must get copies of these reports turned over to State ITAs, if they have a State ITA, or if they are a large jurisdiction buying a voting system, that it needs to be part of their contract with the vendor, that you don't sell a product here unless we see a copy of this report, or have it reviewed by somebody that is willing to do a confidentiality agreement.

I agree that it has not been, it has been the most disconcerting of everything we have done, because of the fact that there has been so little funding available for us to be able to go out and do this on our own, it was necessary for the vendor to pay for this process, and it has been a very expensive process, at least if you listen to them screaming and hollering. And so, that product becomes their property, but that in no way means that a State or a jurisdiction

cannot get their hands on this report if they go through the right process to do so, and we have encouraged them to do that.

Chairman EHLERS. Thank you very much. Just a few other comments. First of all, I have, over the years as a county commissioner, State house member, State senator, and now here, worked with many county clerks, city clerks, township clerks, and poll workers, and I have to say that by and large, they are the salt of the Earth. They are very dedicated, they really want to do it right, and we have to recognize that. And so, our purpose here is not to condemn them, or to denigrate them, but simply say we want to try to help you to do it right.

We also have to recognize the federal role in elections is Constitutionally limited. We, of course, can worry about federal elections, but there are a lot of other elections, city, township, State, and so forth, that we do not have jurisdiction over, unless there is evidence of fraud that our Justice Department would have to investigate.

So, and it has been a very difficult road to get where we are. I am pleased with where we are, except we should have been here two years ago. But we will get this done, and we will have a safe and secure system to the extent possible.

I, also, with Mr. Gutknecht's comment about fingerprints, I was reminded of an election story—this is true—some years ago, in an unnamed jurisdiction, where the county political boss was in the habit of registering his dog to vote as well as himself, and this became general knowledge, and the people just sort of lived with it. However, he overreached when he registered the dog in three different precincts, and the dog voted in all three precincts. That was the end of the political boss. So, fraud is not exactly new, and not even imaginative.

But it is pleasure to thank you for your participation here. It has been a good hearing, and we are very pleased with the progress. As I say, it is later than we would like, but we are looking for good results, and we hope the next election, Presidential or otherwise, will be far better than it was four years ago.

I thank the panelists for coming here. You have all contributed substantially to the hearing, and I appreciate it. If there is no objection, the record will remain open for additional statements by the Members, and for answers to any follow-up questions that the Subcommittee may ask of the panelists by writing, and we would appreciate it if you would respond to those if we send them to you.

Without objection, so ordered, and the hearing is now adjourned.

[Whereupon, at 4:01 p.m., the Subcommittee was adjourned.]

Appendix:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Carolyn E. Coggins, Director, ITA Services at SysTest Labs

Q1. How do the standards and testing methodologies for voting equipment differ from standards and testing methods for other kinds of equipment that your company tests? Are tests for voting equipment generally more or less specific or comprehensive?

A1. An ITA performs two distinct types of testing on electronic Voting Systems. These are as follows:

1. Software and integrated system testing where the focus is on testing to ensure the functionality, security, accuracy, etc., of either software or firmware.
2. Hardware environmental testing where the focus is on ensuring that custom developed hardware meets all applicable environmental standards.

Hardware Environmental Testing: The standards for this are fairly specific and straightforward, having been derived from the manufacturing industry for hardware components and hardware devices. The methods used for hardware environmental testing are very similar to methods used for testing other kinds of equipment. The requirements within the 2002 Federal Election Commission Voting System Standards, VSS, and methods for hardware environmental testing directly resemble the international standards and many of the standards within the VSS either call out or reference both national and international hardware environmental testing standards, e.g., FCC, OSHA, ISO and Mil standards.

Software and Integrated System Testing: The methods for testing software and integrated systems can be as varied as there are different software applications and industries. In addition, although standards from the FEC (the 2002 VSS), IEEE, the SEI, FDA, DOD, ISO and others exist for software, there is no uniformly adopted testing approach for the software development world. SysTest Labs has a testing methodology that governs our testing processes and procedures. This methodology, Advanced Test Operations Management™ (ATOM™) ensures that SysTest Labs follows the same basic techniques, regardless of the type of system. ATOM™ was audited by the NASED Auditors and approved for use in testing of electronic Voting Systems. Having ATOM™ in place at SysTest Labs ensures that we take a robust and repeatable approach to each and every test effort, from banking systems to electronic Voting Systems. The only difference between our testing of electronic Voting Systems and other systems is in the depth of testing.

The depth of testing for other systems is defined by many factors. SysTest Labs has separated systems into three basic categories related to the criticality or the magnitude of impact/risk of the system. These are:

Low Criticality or Magnitude of Impact/Risk: General Commercial

- Testing is performed to customer requirements.
- Customer assesses the risk and determines if testing is sufficient.
- Testing is often viewed as a cost center item as opposed to a profit center item. Customers or Vendors may try to minimize the time and money spent on testing.
- There are no uniformly adopted standards for these types of systems and the methods for testing can vary from ad hoc (no planning) to extremely systematic and robust.
- Acceptance criteria: Sufficient can be fluid, responding to influences like the benefit of "first to market" and budgets.

Medium Criticality or Magnitude of Impact/Risk (e.g., Electronic VOTING SYSTEMS, Gaming, Telecommunications, Banking, and others)

- Testing can be required to meet regulatory standards with either government or fiduciary oversight.
- Testing is still viewed as a cost center item as opposed to a profit center item. This translates to customers or Vendors trying to minimize the time and money spent on testing.
- Level of testing is determined by financial risk, penalty, or governed by published guidelines and/or standards.
- Acceptance criteria: Customer may set the acceptance criteria or the acceptance criteria may be defined by regulatory standards. The customer may define which requirements the system will meet, i.e., the regulations or stand-

ards do not force the customer to meet all system requirements but a minimum set of requirements.

High Criticality or Magnitude of Impact/Risk: (e.g., DOD, NASA, FDA):

- Life critical systems.
- The systems must meet very stringent standards and requirements.
- The methods used for testing are required to meet very stringent standards and requirements.
- Oversight and enforcement by DOD, NASA or the FDA.
- Comprehensive level of testing determined by class; class defines severity of risk, i.e., life and/or injury.
- Acceptance Criteria: Meets all requirements and standards, must be free of defects. Per the 2002 VSS and NASED guidelines, an ITA is required to ensure that a voting system being tested meets the "minimum requirements of the voting system standards." The VSS specifies what minimum set of requirements a voting system must meet in order to be recommended for qualification. The VSS does not specify an exhaustive set of requirements for software and these requirements tend to be at a very high level leaving significant room for interpretation by both the Vendor and ITA. It is not to say that all voting systems tendered for ITA Qualification only meet the minimum requirements of the VSS. However, it is important to recognize that the intent of the standards is to define a minimum set of requirements that all voting systems must meet in order to be recommended for qualification at a federal level. The individual functionality required by each state is not addressed in the standards other than to task the ITA to test additional functionality to the "Vendor's requirements." This assumes the Vendor designed to the correct requirement.

ITA software and integrated system testing for voting equipment is very specific. All voting systems submitted for testing must pass a standard set of tests based upon the minimum requirements of the VSS, customized to the individual voting system design. However it is generally less comprehensive than testing for other systems. This is, in part, because the VSS requirements stipulate that the Vendor has an internal quality assurance and testing program. ITAs may accept Vendor testing if a review of their pre-submission testing is found to be comprehensive. Unlike other testing we perform, we cannot make recommendations regarding the design of a system. In testing a system we must remain impartial. We can make observations about a design or function that is less than optimal but if it meets the VSS, we cannot withhold a recommendation. Although testing has shown that many Vendors exceed the VSS, when an issue is encountered and there is a dispute between the Vendor and the ITA, the Vendor will assert that the ITA's charter is to hold them to "the minimum requirements of the standards."

Q2. To your knowledge, do the tests used by SysTest to evaluate the performance of voting machines differ from the tests used by the other Independent Testing Authorities? Does NIST need to develop uniform testing procedures that would require every lab to use exactly the same test?

A2. SysTest Labs believes that the hardware environmental tests performed between Wyle Labs and SysTest Labs are virtually the same. Again, these types of tests have been required for hardware components and devices for some time and are standard throughout the industry.

SysTest Labs does not have access to the tests used by Ciber as a Software ITA. Therefore, SysTest Labs cannot provide an objective determination of whether or not our tests differ. SysTest Labs can state that within the last three years, our methods and tests have been reviewed by NASED Auditors (at least four times) and that software testing for our first ITA test effort was closely monitored and observed by the Auditors during late 2001 and early 2002.

Having NIST develop a uniform set of software testing procedures would be very difficult. Each electronic Voting System will have a different approach and solution to meeting the requirements of the VSS. For example, touch screen devices can take the form of small screens, full-face ballots, systems that produce paper ballots from the touch screen, etc. In addition, the solution for election management systems can take many different forms depending on the database, reporting mechanisms, etc. This is the challenge that Software Testing faces when designing tests to ensure that an electronic Voting System meets the requirements of the VSS. The overall objectives will generally be the same, but the specific steps required to test out functionality will vary greatly from system to system. In addition, since there are

requirements within the VSS that are not mandatory, some systems will require tests that others may not (depending on whether or not the Vendor states that they support the optional requirements).

An alternative would be for NIST to work with the ITAs and together, design and develop the following items:

1. Testable scenarios and objectives for ballots, contests, voting, tabulating, etc., or identify *specific* types of tests, configurations, ballots, contests, etc. but allow the ITA lab to control their actual test procedures.
2. Provide State-by-State requirements for handling of voting variations. (Help identify conflicting requirements.)
3. Define and standardize the format, data, and acceptance criteria upon which the ITA must report.

Q3. Besides the recommendations you provided in your testimony on what specific kinds of computing problems need to be addressed by NIST during standards development, are there other activities that NIST could carry out to help the ITAs improve the testing process?

A3. SysTest Labs suggests the following items that NIST could carry out to help the ITAs improve the ITA Qualification Testing process:

1. Issue technical bulletins and clarifications as needed for ITA Qualification Testing.
2. Develop a process for reporting disagreements between the ITA and the Vendors regarding interpretation of the VSS requirements or when an ITA requires a ruling on an issue with a Vendor's system.
3. Standardize the reporting elements. Provide a Qualification Report format and structure that allows "apples to apples" comparisons of reports.
4. Provide state-by-state requirements for handling of voting variations. (Help identify conflicting requirements.) This is not only beneficial to the ITA but providing this information to Vendors will help ensure that they build better voting systems.
5. Recognize and understand that testing of an electronic Voting System is not just the responsibility of the ITA
   - Define what should be considered public information and what should remain proprietary.
   - Provide a basic set of guidelines for testing at state certification and local acceptance testing levels.
   - Provide guidelines and methods to local jurisdictions on the use of ongoing Vendor services for programming and acknowledge that local jurisdictions have responsibilities for performing independent testing or oversight of Vendor ballot programming.
   - A representative from NIST must be required to read and evaluate qualification and certification reports. Include report criteria in the standards so that there is a common output with a focus on providing information that can be used and understood by state and local election officials.
   - Help the EAC to develop a common definition for all functional elements of a voting system including software, hardware, and documents.
   - Help the EAC to define a clear process and timeline for submitted Qualification Report review and acceptance/rejection by the EAC and NIST. (Method of submission, timeframe to review, method of acceptance/rejection, veto, appeals, etc.)
   - Help the EAC to develop a document and library structure as the clearinghouse for Qualified Voting System software and hardware systems.
   - Help the EAC to define the clearinghouse role and identify responsibilities: report retention, source code and executable retention, voting system documentation retention, policy for access to reports, policy for obtaining/tracking results of state certification, and national database to track voting system problem reports.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Hratch G. Semerjian, Acting Director, National Institute of Standards and Technology (NIST)

Q1. To your knowledge, do the test protocols used by testing laboratories to evaluate similar or identical pieces of equipment (not necessarily voting equipment) vary widely among different testing labs, or do they use identical tests? If there is a significant variation, does NIST need to develop uniform testing procedures for voting equipment as part of its responsibilities under the Help America Vote Act.

A1. NIST has no information about the test protocols used in the past by the NASED testing laboratories (ITAs). However, a well-written test protocol is always preferable to a less well-written test protocol. NIST could contribute considerably to the development of test protocols that are within NIST's scope of expertise. The improved test protocols would most likely result in better agreement among EAC accredited laboratories.

In general, when detailed test protocols are used, e.g., the IEC 61000 series (see http://www.iec.ch/about/mission-e.htm), different laboratories would be expected to report equivalent test results and when test protocols are not detailed, it is not possible to determine, in advance, if equivalent test results will be reported. When a test method involves sampling, the results will depend on the sample.

Voting equipment and systems are usually tested four times: during product development, qualification testing, certification testing, and acceptance testing. At each stage, there is the possibility of different test methods being used. In some cases, a different test method must be used, e.g., determination of inter-operability of system components versus conformance of a component to a specification or determination that the system incorporates the laws of a particular locality.

Q2. Mr. Shamos says in his testimony that the performance of a particular machine against national standards is considered proprietary. Should that information be revealed to the public?

A2. Within recognized national and international accreditation programs, accredited laboratories are not permitted to reveal proprietary or confidential information belonging to their clients. A vendor may share a test report that it owns with anyone that it wishes. A laboratory may provide information only if specifically requested to, in writing, by the owner of the information.

Intellectual property rights must be respected. A requirement to reveal information may violate those rights. Unless the specifications, standards, test methods, test results, interpretations, and requirements are all provided, a statement of "performance" would be meaningless and potentially damaging to some or all of the parties involved in the contract.

As the rule-making body under HAVA, the EAC could choose to require the public disclosure of certain information about voting systems as part of an accreditation process. States and localities could do the same. There would have to be publicly available requirements and conditions defining the requirement. The EAC, the States, or localities could require disclosure of information in the contract between vendor and purchaser. That information could, by contract, be declared publicly available or proprietary, again by the EAC and not NIST.

Q3. What laboratories have indicated their interest to NIST in becoming testing laboratories under HAVA and how long do you anticipate the accreditation of these labs to take?

A3. As a matter of procedure, the National Voluntary Laboratory Accreditation Program, NVLAP, does not reveal the names of laboratories that express an interest in NVLAP programs or accreditation *(http://ts.nist.gov/ts/htdocs/210/214/214.htm).*

In August, NIST/NVLAP held an initial workshop to gauge interest within the laboratory community (see: *http://ts.nist.gov/is/htdocs/210/214/whatsnew.htm*). An archived webcast of the workshop is available for viewing at: http://www.eastbaymedia.com/NVLAPworkshop.

Approximately 10 laboratories attended the initial workshop. They were not all voting systems laboratories. They may or may not be interested in becoming accredited. A formal call for interested laboratories will be made shortly. Another workshop will likely follow in the December time frame.

The length of time it takes to accredit laboratories depends on the laboratories and how ready they are to meet ISO 17025 standards for laboratory accreditation. The laboratories must meet the requirements of NIST Handbook 150 (*http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf*) and any program specific

requirements (yet to be developed). Given the complexity of this program, it could well take one year for the laboratories to meet the requirements, be assessed, resolve findings, and receive accreditation. In addition to the writing of program specific requirements, it is necessary to identify and train appropriate assessors. Assessor teams of one or more experts will be assigned for each laboratory. The size and make-up of the assessor team will depend on the scope of accreditation of the laboratory. Because of the uncertainty involved in the accreditation process, the EAC could decide to "grandfather" the current ITAs (laboratories), for a period of time to maintain continuity.